«Утверждено»

Протоколом заседания

Наблюдательного совета акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан»

№ 48 от «27» декабря 2021 г.

Приложение

к Протоколу заседания

Правления акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан»

№ 167 от «24» 12 2021 г.

Рег № 124-6 от 27.12.2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «НАЦИОНАЛЬНЫЙ БАНК ВНЕШНЕЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН»

Ташкент 2021

СОДЕРЖАНИЕ

I. Введение

АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан» (далее – АО «Узнацбанк») организовано для оказания широкого спектра банковских услуги субъектам.

Для реализации своих задач в АО «Узнацбанк» эффективно внедряются и применяются информационно-коммуникационные технологии (ИКТ), на их основе формируется и развивается банковская информационная инфраструктура АО «Узнацбанк». Задача обеспечения информационной безопасности в АО «Узнацбанк» является приоритетной в условиях, когда необходимо обеспечить надежную и бесперебойную работу банковской системы для оказания банковских услуг, а также защиту коммерческой, банковской и персональной информации в соответствии с требованиями законодательства.

Информационная безопасность рассматривается с позиции сохранения конфиденциальности, целостности и доступности защищаемой конфиденциальной информации, включая коммерческую и банковскую тайну, персональные данные сотрудников и клиентов банка, служебную информацию банка, а также обеспечения непрерывного и бесперебойного функционирования эксплуатируемых и внедряемых информационных систем и ресурсов АО «Узнацбанк», включая Интегрированную автоматизированную банковскую систему (ИАБС).

Информационная безопасность достигается путем внедрения и реализации комплекса мер, включающих в себя политики, практики, процедуры и организационные структуры. Комплекс мер по информационной безопасности должен обеспечивать защиту информации (данных) АО «Узнацбанк» и её банковскую информационную инфраструктуру от широкого спектра угроз, с целью обеспечения непрерывной деятельности АО «Узнацбанк», минимизации ущерба от реализации угроз, прогнозирования и предотвращения их воздействия, поддержания деловой репутации и соблюдения требований законодательства.

Политика информационной безопасности АО «Узнацбанк» (далее – Политика) определяет основные принципы по защите её информационных активов и банковской информационной инфраструктуры. Она служит основой для принятия соответствующих документов по построению системы управления информационной безопасности (СУИБ) в АО «Узнацбанк». Настоящая Политика представляет собой совокупность документированных руководящих принципов, правил, процедур и практических методов в области обеспечения информационной безопасности, которыми АО «Узнацбанк» руководствуется в своей деятельности.

Политика информационной безопасности АО «Узнацбанк» согласована со Службой государственной безопасности Республики Узбекистан (письмо №13/16614 от 09.11.2021 г.) и Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан (письмо №27-8/7322 от 15.10.2021 г.).

II. Нормативные ссылки

2.1. Политика информационной безопасности АО «Узнацбанк» разработана в соответствии с нижеследующими нормативными документами по обеспечению информационной безопасности объектов информатизации Республики Узбекистан:

Закон Республики Узбекистан от 11 декабря 2003 года, №560-П«Об информатизации»;

Закон Республики Узбекистан от 5 ноября 2019 года, №580 «О банках и банковской деятельности»,

Закон Республики Узбекистан от 4 апреля 2006 года, №ЗРУ-30 «О защите информации в автоматизированной банковской системе»;

Закон Республики Узбекистан от 1 ноября 2019 года, №ЗРУ-578 «О платежах и платежных системах»;

Закон Республики Узбекистан от 11декабря 2003года №562-II «Об электронной цифровой подписи»;

Закон Республики Узбекистан от 29 апреля 2004 года №611-II «Об электронном документообороте»;

Закон Республики Узбекистан от 11 сентября2014 года№374 «О коммерческой тайне»;

Закон Республики Узбекистан от 30 августа 2003 года №530-II «О банковской тайне»;

Закон Республики Узбекистан от 9 декабря2015 года№395 «Об электронном правительстве»;

Закон Республики Узбекистан от 2 июля 2019 года №ЗРУ-547 «О персональных данных»;

Постановление Президента Республики Узбекистан от 3 апреля 2007 года №ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан»;

Постановление Президента Республики Узбекистан от 8 июля 2011 года №ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;

Постановление Президента Республики Узбекистан от15 июня 2020 года №ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан»;

Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах»;

Постановление Кабинета Министров Республики Узбекистан от 7 ноября 2011 года №296 «О мерах по реализации постановления от 8 июля 2011 года №ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;

Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан»;

Постановление Министерства внутренних дел и Правления Центрального банка Республики Узбекистан от 5 июня 2010 года №12, 22/7-ДСП «Об утверждении инструкции об организации охраны банков и их филиалов подразделениями охраны при органах внутренних дел Республики Узбекистан»;

Постановление Правления Центрального банка Республики Узбекистан от 25 января 2020 года №2/4 «Об утверждении Положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан», зарегистрировано Министерством юстиции Республики Узбекистан 10 марта 2020 года рег. №3224;

Постановление Правления Центрального банка Республики Узбекистан «Об утверждении Положения об обеспечении информационной безопасности в платежных системах операторов платежных систем и поставщиков платежных услуг», зарегистрировано Министерством юстиции Республики Узбекистан 30 июня 2020 года рег. №3268;

O‘zDSt ISO/IEC 27000:2014 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь»;

O'zDSt ISO/IEC 27001:2016 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;

O'zDSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасности»;

O‘zDSt ISO/IEC 27003:2014 «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью»;

O‘zDSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности»;

O‘zDSt ISO/IEC 27007:2015 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью»;

O‘zDSt ISO/IEC 27008:2015 «Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления информационной безопасностью»;

O‘zDSt ISO/IEC 27010:2015 «Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями»;

O‘zDSt ISO/IEC 27014:2018 «Информационная технология. Методы обеспечения безопасности. Корпоративное управление информационной

безопасностью»;

O‘zDSt ISO/IEC 27031:2016 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса»;

O‘zDSt ISO/IEC 27032:2017 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по кибербезопасности»;

O‘zDSt ISO/IEC 27033-1:2016 «Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции»;

O‘zDSt ISO/IEC 27033-4:2016 «Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности»;

O‘zDSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами»;

O‘zDSt 3387:2019 (ISO/IEC 27035-2:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию и подготовке к реагированию на инциденты»;

O‘zDSt 1047:2018 «Информационная технология. Термины и определения»;

O‘zDSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения;

O‘zDSt 1109:2013 «Информационная технология. Криптографическая защита информации. Термины и определения»;

O‘zDSt ISO/IEC 15408-:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»;

O‘zDSt ISO/IEC 15408-:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»;

O‘zDSt ISO/IEC 15408-:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»;

O‘zDSt ISO/IEC 13335-:2009 «Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий (часть 1). Концепции и модели управления безопасностью информационно-коммуникационных технологий»;

O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;

O‘zSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации»;

O‘zDSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия не декларированных возможностей»;

O‘zDSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации»;

OzDSt 2875:2014 «Требования к дата-центрам. Обеспечение инфраструктуры и информационной безопасности»;

O‘zDSt 081: 1092:2009 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

O‘zDSt 081 1108:2011 «Информационная технология. Взаимосвязь открытых систем. Структура сертификата открытого ключа ЭЦП и сертификата атрибута»;

RH 45-015:2016 «Унифицированные системы документации. Организационно-распорядительная документация. Виды, состав и оформление»;

RH 45–170:2004 «Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей»;

Инструкция о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения, утвержденная 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан – председателем межведомственной комиссии по вопросам защиты государственных секретов;

Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан (Приложение №10 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно коммуникационной системы Республики Узбекистан на 2013-2020 годы от 23 февраля 2016 года № 7);

Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности (приложение №1 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от17 ноября 2017года №7);

Требования обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах (Приложение №2 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от 17 ноября 2017 года №7).

III.Термины и определения

3.1. В настоящей Политике применены термины согласно государственному стандарту O`zDst 2927:2015 «Информационная безопасность. Термины и определения». Также в тексте встречаются термины с соответствующими определениями:

анализ рисков: систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам;

база данных: совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ;

банковская тайна: защищаемые банком сведения:

- об операциях, счетах и вкладах своих клиентов (корреспондентов);
- о своем клиенте (корреспонденте), полученные банком в связи с оказанием ему банковских услуг;
- о наличии, характере и стоимости имущества клиента (корреспондента), находящегося на хранении в сейфах и помещениях банка;
- о межбанковских операциях и сделках, совершенных по поручению клиента (корреспондента) или в его пользу;
- о клиенте (корреспонденте) другого банка, ставшие известными в результате обращения сведений, составляющих банковскую тайну, между банками;

безопасность информации: состояние защищенности информации, обрабатываемой средства вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;

виртуальная частная сеть (VPN): представляет собой подключение типа (точка-точка) в частной или общедоступной сети, например, в Интернете. VPN-клиенты используют специальные TCP/IP протоколы, называемые туннельными протоколами, обеспечивающие установление защищенного канала обмена данными между двумя компьютерами;

документированная информация: зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать;

злоумышленник (нарушитель): лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и ее ресурсам и совершившие преднамеренные действия для их несанкционированного получения или изменения;

информационный ресурс: отдельные документы, отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других);

информационная система: организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией;

информация ограниченного доступа: документированная

информация, содержащая сведения, составляющие государственные секреты и конфиденциальную информацию, доступ к которой ограничивается в соответствии законодательством;

инцидент информационной безопасности: единичное событие или ряд нежелательных, или непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации защищаемой информации и реализации угрозы информационной безопасности;

коммерческая тайна: информация, имеющая коммерческую ценность в научно-технической, технологической, производственной, финансово-экономической и других сферах в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и собственник этой информации принимает меры по защите ее конфиденциальности;

контролируемая зона: пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

Примечание: Граница контролируемой зоны могут быть:

- периметр контролируемой территории организации;
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;

конфиденциальная информация: документированная информация, не содержащая сведений, составляющих государственные секреты, доступ к которой ограничивается в соответствии с законодательством;

корпоративная сеть: информационно-вычислительная сеть, объединяющая локальные сети отдельных предприятий (фирм, организаций, акционерных обществ и т.п.) корпорации в масштабе как одного государства, так и нескольких государств;

локальная вычислительная сеть (ЛВС): информационно-вычислительная сеть, связывающая ряд устройств вычислительной техники в одной локальной зоне, ограниченной зданием или одним предприятием;

несанкционированный доступ: доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа;

объект информатизации: информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, а также отдельные помещения, предназначенные для ведения переговоров в т.ч, конфиденциальные;

оценка рисков: процесс сравнения рассчитанного риска и критериев риска, выполняемый с целью определения его значения;

персональные данные: сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

политика безопасности: набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного подмножества объектов и субъектов безопасности;

программное обеспечение: совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ;

риск: возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы;

сервер: совокупность аппаратного и программного обеспечения (программа-сервер), позволяющая компьютеру предоставлять услуги другому компьютеру. Компьютеры работают с программой-сервером с помощью программ-клиентов;

система управления информационной безопасностью: часть общей системы управления, основанная на использовании методов оценки бизнес-рисков, предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, обслуживания и совершенствования информационной безопасности;

системный администратор: должностное лицо, назначенное в установленном порядке, ответственное за эксплуатацию службы каталога, систем управления базами данных и прочих систем или серверов, их ведение, настройку, изменение полномочий пользователей, информационную безопасность;

средства защиты информации: технические, криптографические и другие средства, предназначенные для защиты информации, в том числе средства контроля эффективности защиты информации;

угроза: потенциальная возможность нарушения компьютерной безопасности;

уязвимость: недостаток в системе обработки данных, используя который, можно нарушить ее целостность и вызвать неправильную работу.

IV. Обозначения и сокращения

4.1. В настоящей Политике применены следующие обозначения и сокращения:

IDPS (Intrusion Detection & Prevention System) – средства (система) обнаружения и предотвращения вторжений;

SAN (Storage Area Network) – сеть хранения данных;

SIEM (Security Information and Event Management) – система управления инцидентами информационной безопасности;

SWIFT (Society for Worldwide Interbank Financial Telecommunications)- Общество всемирных межбанковских финансовых каналов телекоммуникаций;

VISA/MasterCard– международные платежные системы, предоставляющие услуги проведения платёжных операций;

VPN (Virtual Private Network) - виртуальная частная сеть;

UPS (Uninterruptible Power Supply) – источник бесперебойного питания;

БИС – банковская информационная система АО «Узнацбанк»;

ВОЛС - волоконно-оптическая линия связи;

ДИББ - Департамент информационной и банковской безопасности (подразделение головного офиса АО «Узнацбанк»);

ДИТ - Департамент информационных технологий (подразделение головного офиса АО «Узнацбанк»).

ДРБ - Департамент розничного бизнеса (подразделение головного офиса АО «Узнацбанк»);

ИАБС – Интегрированная автоматизированная банковская система АО «Узнацбанк»;

ИКТ - информационно-коммуникационные технологии;

ЛВС - локальная вычислительная сеть;

МСПД – межведомственная сеть передачи данных;

ПО – программное обеспечение;

СКЗИ – средства криптографической защиты информации;

СКУД – система контроля управления доступа;

СУБД – система управления базой данных;

СУИБ - система управления информационной безопасностью;

УИБ - Управление информационной безопасности (структурное подразделение ДИББ);

ЦОД – центр обработки данных;

ЭЦП – электронная цифровая подпись.

V.Область применения

5.1. Политика информационной безопасности АО «Узнацбанк» определяет цели и задачи защиты, правила, процедуры, практические приёмы и руководящие принципы в области информационной безопасности, которыми руководствуется АО «Узнацбанк» в своей деятельности. В Политике информационной безопасности АО «Узнацбанк» рассмотрены основные принципы построения, организационные, технологические, процедурные и иные аспекты обеспечения информационной безопасности в АО «Узнацбанк».

5.2. Политика информационной безопасности АО «Узнацбанк» должна использоваться АО «Узнацбанк» в качестве основы для построения комплексной СУИБ в АО «Узнацбанк», включая разработку внутренних нормативных документов, принятие организационных, технических и иных мер обеспечения информационной безопасности.

5.3. Требования настоящей Политики распространяются на всю защищаемую информацию АО «Узнацбанк» и средства обработки, хранения и передачи этой информации, за исключением сведений, содержащих государственные секреты. Защита информации, содержащей государственные секреты, обеспечивается в соответствии с законодательством.

5.4. Соблюдение настоящей Политики обязательно для всех работников АО «Узнацбанк»:

- головного офиса (правление, департаменты, управления, иные структурные подразделения) АО «Узнацбанк»;

- филиал Главного управления по Ташкенту (ОПЕРУ-операционное управление, ГОПЕРУ – главное операционное управление, ЦОФ-центральный операционный филиал);

- 13 региональных филиалов (филиал Республики Каракалпакстан, Андижанский областной филиал, Бухарский областной филиал, Джизакский областной филиал, Кашкадарьинский областной филиал, Навоийской областной филиал, Наманганский областной филиал, Самаркандский областной филиал, Сурхандарьинский областной филиал, Сырдарьинский областной филиал, Ташкентский областной филиал, Ферганский областной филиал, Хорезмский областной филиал);

- районных филиалов Главного управления по Ташкенту и региональных филиалов;

- Центров оказания услуг населению и минибанков АО «Узнацбанк», организуемых при региональных и районных филиалах.

Входящие в структуру АО «Узнацбанк» подведомственные организации (ООО «NBU InvestGroup», АО «Азия-Инвест Банк») имеют собственную Политику информационной безопасности, направленные на защиту имеющихся у них информационных систем и ресурсов.

5.5. Требования настоящей Политики распространяются на все информационные системы и ресурсы АО «Узнацбанк», на всех сотрудников АО «Узнацбанк» и его региональных филиалов (штатных, временных, работающих по контракту и др.), вне зависимости от места их работы и занимаемой должности, на третьих лиц, взаимодействующих с АО «Узнацбанк» (поставщики, подрядчики, аудиторы, оценщики, посетители, обслуживающий персонал и т.п.), которые по тем или иным причинам имеют легитимный доступ к информационным ресурсам и системам АО «Узнацбанк».

5.6. Руководители подразделений головного офиса, филиала Главного управления по Ташкенту и региональных филиалов (далее – областные филиалы АО «Узнацбанк»), районных филиалов АО «Узнацбанк» должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, Департамент информационной и банковской безопасности (ДИББ) проводит периодическую проверку соблюдения требований настоящей Политики с представлением отчета по результатам указанной проверки руководству правления АО «Узнацбанк».

VI.Цели и задачи

6.1. Основной целью Политики информационной безопасности АО «Узнацбанк» является выработка комплексных подходов, принципов, правил, процедур и практических мер, направленных на:

- защиту субъектов информационных отношений, в частности клиентов АО «Узнацбанк», от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования объектов информатизации АО «Узнацбанк» или

несанкционированного доступа к циркулирующей в ней информации и её незаконного использования;

- обеспечение соблюдения требований законодательства, руководящих и нормативных документов в области обеспечения информационной безопасности;

- сохранение конфиденциальности, целостности и доступности деловой, коммерческой, банковской, платежной и персональной информации АО «Узнацбанк»;

- обеспечение непрерывного и бесперебойного функционирования информационных системы и иных объектов информатизации, включая банковские и платежные системы АО «Узнацбанк», обеспечивающие деятельность банка и оказание им банковских услуг клиентам;

- соблюдение соответствие стандарта безопасности платежных карт PCI DSS, а также иных банковских карт АО «Узнацбанк»;

- устранение и минимизация возможных последствий инцидентов информационной безопасности, прогнозирование, предотвращение и пресечение реализации угроз, выявление и устранение уязвимостей на объектах информатизации и СУИБ;

- формирование комплекса организационно-технических мероприятий по обеспечению информационной безопасности и бесперебойного устойчивого функционирования единой электронной информационно-аналитической системы государственной гражданской службы, ресурсов и баз данных АО «Узнацбанк», с учетом широкого спектра угроз;

- обеспечение резервирования информационных систем и систем восстановления данных;

- обеспечение резервирования систем жизнеобеспечения»;

6.2. Политика информационной безопасности АО «Узнацбанк» должна решать следующие задачи:

- определение объектов защиты и их классификация по уровню защищенности в соответствии с государственным стандартом O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;

- распределение обязанностей и ответственности между структурными подразделениями АО «Узнацбанк» по обеспечению информационной безопасности;

- разработка единых требований, предъявляемых к информационным технологиям, применяемым в банковской информационной инфраструктуре АО «Узнацбанк» с точки зрения информационной безопасности;

- создание и развитие СУИБ АО «Узнацбанк», обеспечивающей комплексный подход обеспечения информационной безопасности с применением организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации;

- формирование комплекса организационно-технических мероприятий по обеспечению информационной безопасности и бесперебойного устойчивого

функционирования информационных систем, ресурсов и баз данных, с учетом широкого спектра угроз;

- своевременное выявление и прогнозирование внутренних и внешних угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

- выявление и устранение уязвимостей в информационно-коммуникационной инфраструктуре и СУИБ АО «Узнацбанк»;

- создание условий для максимальной минимизации ущерба от реализации угроз информационной безопасности на объектах информатизации»;

- определение процедур оперативного реагирования на возникшие угрозы безопасности информации и негативные инциденты;

- обеспечение контроля за конфиденциальностью, целостностью и доступностью объектов защиты и защищаемой информации;

- повышение квалификации кадров в области защиты информации и осведомленности сотрудников АО «Узнацбанк» в области рисков информационной безопасности.

- соблюдения соответствия стандарта безопасности платёжных карт PCIDSS.

VII.Основные положения

7.1. Настоящая Политика предусматривает обеспечение информационной безопасности на основе использования совокупности правовых организационных, технических и других методов и средств защиты информации, а также осуществления всестороннего непрерывного контроля эффективности реализованных мер в области информационной безопасности.

7.2. Политика информационной безопасности АО «Узнацбанк» основывается на следующих основных принципах:

- законность - соблюдение Конституции и законодательства Республики Узбекистан, законных прав пользователей, реализация мер обеспечения информационной безопасности в строгом соответствии с действующим законодательством и требованиями нормативных актов;

- вовлеченность и персональная ответственность – в процессе обеспечения информационной безопасности участвуют руководство и все сотрудники АО «Узнацбанк», и они несут персональную ответственность за соблюдение требований информационной безопасности, которые включаются в трудовые договора и должностные инструкции работников, а также в договора (соглашения) с контрагентами;

- осведомленность и знание сотрудников - требования в области информационной безопасности доводятся до сведения сотрудников АО «Узнацбанк» в части их касающейся, на периодической основе осуществляется информирование, обучение и аттестация сотрудников по вопросам обеспечения информационной безопасности, повышение квалификации специалистов, ответственных за обеспечение информационной безопасности (на курсах,

вебинарах, тренингах, семинарах в области обеспечения информационной безопасности);

- взаимодействие и согласованность действий - действия по обеспечению информационной безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений и согласованы между собой по целям, задачам, принципам, методам и средствам;

- системный подход - учет при построении СУИБ всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности;

- комплексность – используемые разнородные методы и средства защиты должны в совокупности организовывать целостную систему защиты от всевозможных угроз, не содержащей слабых мест и обеспечивающую эшелонированную защиту всех защищаемых объектов;

- непрерывность защиты – процесс обеспечения информационной безопасности должен быть постоянным по времени и идти на всех уровнях АО «Узнацбанк»;

- экономическая целесообразность - меры обеспечения информационной безопасности выбираются с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации;

- подконтрольность и учет действий – контроль выполнения принятых требований информационной безопасности сотрудниками, предоставление и управление доступом сотрудников к информационным активам, ведение учета всех действий сотрудников с информационными активами АО «Узнацбанк».

7.3. АО «Узнацбанк» в процессе реализации своих задач по обеспечению информационной безопасности:

- формирует нормативную базу, регламентирующие процессы по обеспечению информационной безопасности банковской информационной инфраструктуры АО «Узнацбанк»;

- определяет и категорирует информацию и иные объекты защиты АО «Узнацбанк»;

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности, анализ и оценку рисков;

- разрабатывает требования и меры по обеспечению безопасности информации банковской информационной инфраструктуры АО «Узнацбанк»;

- организует работу необходимых подразделений по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности;

- осуществляет и обеспечивает контроль за внедрением, развитием, использованием средств защиты информации посредством их сертификации и лицензирования деятельности в области информационной безопасности;

- периодически проводит оценку состояния защищенности информационных активов, выявляет, учитывает и оперативно реагирует на

действительные, предпринимаемые и вероятные нарушения информационной безопасности.

VIII.Объекты защиты

8.1. Основными объектами информационной безопасности АО «Узнацбанк», подлежащие защите, являются:

8.1.1. Конфиденциальная информация АО «Узнацбанк», включая:

- служебную (деловую) информацию АО «Узнацбанк»;
- информацию, составляющую коммерческую тайну АО «Узнацбанк», его клиентов и партнеров, контрагентов, с которыми имеются соглашения и договора;
- информацию, составляющую банковскую тайну в банковской системе АО «Узнацбанк»;
- персональные данные сотрудников АО «Узнацбанк» и его клиентов;
- платежную информацию и документы платежных систем.

8.1.2. Персонал:

- клиенты АО «Узнацбанк»;
- работника банка АО «Узнацбанк».

8.1.3. Рабочие станции, сервера, хранилища данных (системы хранения данных) и иные средства обработки и хранения информации.

8.1.4. Банкоматы, киоски, платежные терминалы и электронные платежные устройства.

8.1.5. Программное обеспечение: операционные системы, прикладное программное обеспечение и приложения, исходные коды, системы управления базами данных (СУБД), диагностические программы, инструментальные средства разработки и утилиты.

8.1.6. Сервисы и системы обмена информации, включая:

- корпоративную электронную почту;
- систему электронного документа оборота АО «Узнацбанк»;
- систему IP-телефонии для организации корпоративной телефонной связи между головным офисом, областными и районными филиалами, минибанками;
- систему видеоконференцсвязи с организацией селекторных залов в головном офисе и региональных филиалах и с использованием видеотелефонов в районных филиалах;
- защищенную электронную почту E-xat и систему контроля исполнительской дисциплины E-ijro.

8.1.7. Сетевая инфраструктура:

- корпоративная сеть АО «Узнацбанк»;
- внешние каналы подключения и организации корпоративной сети;
- локальные вычислительные сети (ЛВС) головного офиса, региональных и районных филиалов и минибанков,
- сетевое оборудование (маршрутизаторы, таблицы маршрутизации, управляемые и неуправляемые коммутаторы, шлюзы доступа, частные виртуальные сети VPN, модемы), входящие в состав корпоративной сети и

ЛВС.

8.1.8. Информационные ресурсы, включающие:

- файловые сервера FTP в головном офисе, региональных и районных филиалах;

- официальный веб-сайт АО «Узнацбанк» https://nbu.uz/;

- базы данных информационных систем АО «Узнацбанк», а также их электронные архивы.

8.1.9. носители защищаемой информации, в том числе носители ключевой информации (носители криптографических ключей шифрования и ЭЦП, предназначенные для осуществления криптографической защиты информации);

8.1.10. Банковские информационные системы: ИАБС и банковская информационная система (БИС).

8.1.11. Защищаемые помещения, включая:

- основной и резервный ЦОД АО «Узнацбанк» и его помещения;

- коммутационные помещения в региональных и районных филиалах, в которых размещаются маршрутизатор для подключения к корпоративной сети, основной коммутатор ЛВС и файловый сервер FTP;

- помещения, в которых осуществляется обработка конфиденциальной информации в головном офисе, региональных и районных филиалах.

8.1.12. Средства защиты информации (межсетевые экраны, средства организации VPN, средства антивирусной защиты, прокси-сервера, СКЗИ и др.).

8.1.13. Центр регистрации ключей ЭЦП АО «Узнацбанк», обеспечивающий формирование ключей и сертификатов ключей ЭЦП для сотрудников банка и клиентов, пользующихся Интернет-банкингом и мобильным банкингом.

8.1.14. Нематериальные активы.

8.2. Перечень защищаемой конфиденциальной информации определен в приложении №1 к Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан». В данной Инструкции определены порядок формирования перечня конфиденциальной информации, порядок доступа к ней сотрудников банка, порядок работы с конфиденциальной информацией, требования к помещениям, где обрабатывается конфиденциальная информация, и ответственность за нарушение режима работы с конфиденциальной информацией.

8.3. Основными объектами информатизации АО «Узнацбанк», подлежащими обеспечению информационной безопасности, являются:

8.3.1. Интегрированная автоматизированная банковская система (ИАБС) – система для осуществления банковских платежей клиентов АО «Узнацбанк» с входящим в его состав аппаратно-программным комплексом, включая:

- сервера базы данных и системы хранения данных;

- сервера веб-приложений https://milliy.nbu.uz/ и https://ibank.nbu.uz/ для оказания услуг Интернет-банкинг соответственно физическим и юридическим

лицам, являющимся клиентами банка, через сеть Интернет;

- сервера веб-приложения https://iabs.nbu.local/ibs для доступа сотрудников банка к ИАБС через корпоративную сеть;

- сервера приложений (агенты API) для взаимодействия ИАБС с внешними системами Anor и NIBBD Центрального банка Республики Узбекистан и международной системой SWIFT, внутренней системой процессинга для обслуживания клиентов VISA/MasterCard-карт, а также с мобильными приложениями Milliy application клиентов мобильного банкинга.

8.3.2. Банковская информационная система (БИС) – система используется только для формирования банковской отчетности для сотрудников банка во взаимодействии с ИАБС и включает в себя следующий аппаратно-программный комплекс:

- сервер базы данных и система хранения данных;

- сервер веб-приложения https://bisnbs2.local/ для доступа сотрудников банка в БИС через корпоративную сеть.

БИС взаимодействует с ИАБС для получения данных, необходимых для формирования отчетности.

8.3.3. Система процессинга для обслуживания клиентов VISA/MasterCard-карт (далее – система процессинга VISA/MasterCard), включающий в себя следующий аппаратно-программный комплекс:

- сервер обработки процессов VISA/MasterCard-карт (далее – процессинговый сервер VISA/MasterCard), подключаемый по отдельному международному каналу передачи данных к международной системе VISA/MasterCard;

- модемы, VPN-шлюз и маршрутизаторы для подключения банкоматов VISA/MasterCard-карт к системе процессинга VISA/MasterCard);

- банкоматы VISA/MasterCard-карт.

- Центр персонализации карт VISA\MasterCard в мини-процессинговых центрах в филиалах АО «Узнацбанк».

8.3.4. Система электронного документооборота АО «Узнацбанк»- система предназначена для внутреннего электронного документооборота, учета кадров и формирования заявок со стороны сотрудников банка.

8.3.5. Корпоративная сеть АО «Узнацбанк», включающая в себя:

- сервер домена для организации единой ЛВС в АО «Узнацбанк»;

- коммутаторы ядра сети;

- маршрутизаторы для подключения головного офиса и основного ЦОД, резервного ЦОД, региональных и районных филиалов к корпоративной сети;

- маршрутизатор для подключения корпоративной сети АО «Узнацбанк» к внешней сети (Интернет, TAS-IX, МСПД);

- каналы для организации корпоративной сети и подключения к внешним сетям (Интернет, TAS-IX, МСПД) и внешним системам (VISA/MasterCard, Anor, NIBBD, SWIFT);

- коммутаторы и кабеля для организации ЛВС в головном офисе, основном и резервном ЦОД, региональных и районных филиалах, минибанках;

- сеть хранения данных SAN, организуемая между серверами базы

данных и системами хранения данных ИАБС основного и резервного ЦОД;

- собственная ВОЛС между основным и резервным ЦОД;

- собственные каналы связи, используемые для подключения банкоматов банковских карт Uzcard и Humo к корпоративной сети.

8.3.6. Официальный веб-сайт АО «Узнацбанк» https://nbu.uz/, который размещен на хостинг-площадке отдельного провайдера.

8.3.7. Корпоративная электронная почта и почтовый сервер Windows Exchange.

8.3.8. Система IP-телефонии с аппаратно-программным сервером.

8.3.9. Система видеоконференцсвязи с аппаратно-программным сервером.

8.3.10. Основной и резервный ЦОД АО «Узнацбанк».

8.4. Для каждого вышеуказанного объекта информатизации АО «Узнацбанк» составляется технический паспорт в соответствии с требованиями постановления Кабинета Министров Республики Узбекистан от 16.10.2015г. №295.

8.5. В соответствии с государственным стандартом O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации» ИАБС АО «Узнацбанк» имеет класс защищенности 2А.

8.6. ИАБС АО «Узнацбанк» также взаимодействует (обменивается данными) со следующими информационными системами:

1) Anor - автоматизированная система межбанковских платежей Центрального банка Республики Узбекистан;

2) NIBBD - система регистрации счетов юридических и физических лиц, расположенная в Центральном банке Республике Узбекистан (Главный центр информатизации - ГЦИ);

3) международная система SWIFT – система осуществления валютных операций и международных платежей;

4) система процессинга VISA/MasterCard - обработка запросов сотрудников банка, клиентов Интернет-банкинга и мобильного банкинга, связанные с VISA/MasterCard картами.

С вышеуказанными информационными системами ИАБС АО «Узнацбанк» интегрируется через сервер приложений (агент API), обеспечивающие взаимодействие программных комплексов систем и обмен данным между ними. Подключение к системам Anor и NIBBD осуществляется по сети передачи данных ГЦИ Центрального банка Республики Узбекистан.

8.7. Для подключения к международной системе SWIFT в АО «Узнацбанк» организуются основной и резервный процессинговые сервера, размещенные в основном и резервном ЦОД АО «Узнацбанк». Указанные сервера подключаются к международной системе SWIFT по отдельному международному каналу передачи данных. Взаимодействие между процессинговым сервером SWIFT АО «Узнацбанк» и ИАБС через отдельно организованный сервер приложений (агент API).

IX. Риски и модель угроз информационной безопасности

9.1. Модель угроз информационной безопасности АО «Узнацбанк» определяется для каждого важного и критичного объекта защиты и включается в себя:

- описание объекта защиты;
- перечень и описание возможных угроз безопасности для объекта защиты;
- модель нарушителя;
- возможные уязвимости;
- способ реализации угроз;
- последствия от реализации угроз.

9.2. Модель угроз информационной безопасности АО «Узнацбанк» включает в себя следующие основные угрозы информационной безопасности по способу воздействия:

- компьютерно-технические угрозы;
- физические угрозы;
- угрозы с использованием технических каналов утечки информации;
- техногенные угрозы, включая угрозы природного характера;
- организационные и правовые (юридические) угрозы.

9.3. Источники угроз информационной безопасности могут быть внутренними (источник угроз внутри системы АО «Узнацбанк») и внешними (источник угроз вне системы АО «Узнацбанк»).

9.4. Компьютерно-технические угрозы реализуются посредством сетевого взаимодействия на объект защиты и/или с использованием программ, компьютерных средств, а также уязвимостей в них. К компьютерно-техническим угрозам также входят технические отказы.

9.5. Компьютерно-технические угрозы по характеру воздействия делятся на:

- информационные – распространение нежелательной, недостоверной, противоречащей деятельности АО «Узнацбанк» информации в электронном виде, а также нежелательный контент (фишинг), направленный на кражу персональной и конфиденциальной финансовой информации;
- программные – вредоносные программы, использование специализированных программ (шпионское ПО) или не декларированных функциональных возможностей (закладок) в программах;
- сетевые – сетевые атаки и воздействия, использующие уязвимости в сети, сетевых протоколах, программах и средствах, а также применяющие каналы передачи информации и специальные программные средства, которые направлены на получение несанкционированного доступа для кражи, уничтожения или изменения информации, совершения противоправных действий, нарушение нормального функционирования;
- отказы в обслуживании технических и программных средств – выход из строя или нарушение функционирования из-за морального износа или совершения ошибок со стороны обслуживающего персонала или воздействия

на него нарушителя.

9.6. Объектами воздействия компьютерно-технических угроз являются: информация (данные) АО «Узнацбанк» в электронном виде, прикладные и системные программы, средства обработки, хранения и передачи информации, ЛВС и корпоративная сеть, веб-ресурсы банка, файловые хранилища и базы данных информационных систем, информационные системы, включая систему корпоративной электронной почты, ИАБС и др.

9.7. Физические угрозы реализуются посредством физического доступа, физического взаимодействия (воздействия) нарушителя на объект защиты;

Физические угрозы могут быть направлены на:

- уничтожение или разрушение;
- вывод из строя или нанесение вреда;
- совершение противоправных операций;
- хищение (кражу).

К физическим угрозам также относится утечка конфиденциальной информации, полученной путем прямого физического доступа к объекту информатизации и/или информации.

9.8. Объектами воздействия физических угроз являются: информация в электронном виде и документированная информация, носители информации, каналы связи, технические средства обработки, хранения и передачи информации и входящие в них программное обеспечение, помещения, шкафы и сейфы, иные материальные активы, входящие в банковскую информационную инфраструктуру АО «Узнацбанк».

9.9. Угрозы с использованием технических каналов в основном направлены на утечку информации, а также могут быть использованы для воздействия и подавления технических средств и каналов связи. В качестве технических каналов утечек используются: электромагнитные сигналы, в том числе побочные электромагнитные излучения и наводок технических средств и каналов связи, акустические и виброакустические сигналы, электрические сигналы и радиоизлучения, оптические (телевизионные, фотографические и визуальные) сигналы в видимом, инфракрасном и ультрафиолетовом диапазонах волн.

9.10. Объектами воздействия угроз с использованием технических каналов являются: информация в электронном виде, технические средства обработки и хранения информации и каналы связи.

9.11. К техногенным угрозам относятся пожары, взрывы, обрушения сооружений, затопления и иные бедствия, в том числе возникших в результате стихийных природных явлений, которые могут повлечь к уничтожению или разрушению, выводу из строя или нанесению вреда информационным и материальным активам, банковской информационной инфраструктуре АО «Узнацбанк».

Воздействию техногенных угроз подвержены все объекты защиты АО «Узнацбанк».

9.12. К организационным и правовым (юридическим) угрозам относятся нарушения требований законодательства и нормативной базы, регламента и

требований по эксплуатации, выполнение неразрешенных действий персоналом, нарушение юридических прав, нелегальное использование программ и информационных материалов, невыполнение контрактных обязательств и т.д.

Объектами воздействия организационных и правовых угроз являются материальные и нематериальные (имидж) активы АО «Узнацбанк».

9.13. Для определения актуальности угроз информационной безопасности для каждого объекта защиты используются два критерия:

- опасность угрозы;
- возможность возникновения и реализации угрозы.

9.14. Опасность угрозы оценивается исходя из последствий, которые возникнут в результате реализации угрозы и имеет значения:

- высокая – сильные последствия;
- средняя – умеренные последствия;
- низкая – с низкими последствиями.

9.15. Возможность возникновения и реализации угрозы имеет следующие значения:

- высокая - наличие уязвимости и отсутствие методов и средств защиты от угрозы, распространённость угрозы в информационном пространстве;
- средняя - наличие уязвимости в программном обеспечении, применение менее эффективных методов и средств защиты информации, угроза не имеет широкого распространения в информационном пространстве;
- низкая – отсутствие уязвимости, использование средств защиты, реализация угрозы имеет частный случай.

9.16. При разработке модели угроз информационной безопасности для объектов защиты должны учитываться только актуальные угрозы.

Актуальность угрозы информационной безопасности определяется по следующим правилам, приведенным в таблице №1.

Таблица №1. Правила определения актуальности угроз информационной безопасности

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	-	-	актуальная
Средняя	-	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

9.17. В целях определения уровня обеспечения информационной безопасности проводится анализ и оценка рисков. Риски определяются вероятностью причинения ущерба и потерь в случае реализации угроз информационной безопасности. Риски возникают вследствие наличия реальной угрозы воздействия на объект защиты.

9.18. Для деятельности АО «Узнацбанк» существуют следующие основные риски:

- нарушение функционирования (вывод из строя, уничтожение или хищение) объектов защиты в результате несанкционированного доступа к ним нарушителей или неавторизованных пользователей, воздействия на них вредоносных программ, реализации сетевых атак, ошибок действия персонала или ошибки программы, технические отказы;
- нарушение конфиденциальности и целостности защищаемой информации, распространение недостоверной и противоречащей информации;
- совершение противоправных действий и незаконных финансовых операций, финансовые мошенничества.

9.19. Последствиями этих рисков являются:

- приостановка оказания банковских услуг или некачественное их предоставление;
- нарушение непрерывности деятельности АО «Узнацбанк», выполнение им отдельных задач или нарушение непрерывности выполнения отдельных информационно-технологических и производственно-технологических процессов;
- финансовые потери АО «Узнацбанк»;
- раскрытие коммерческой, банковской, персональной тайны и иной конфиденциальной информации;
- нанесение морального и материального (финансовые потери) ущерба клиентам;
- нанесение вреда имиджу и репутации АО «Узнацбанк».

9.20. Анализ и оценка рисков в АО «Узнацбанк» проводится в соответствии с государственным стандартом O‘zDSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности». Анализ и оценка рисков проводится в отношении каждого важного и критичного объекта защиты. Согласно стандарту, при оценке рисков учитывается:

- ценность объекта защиты (стоимость, важность) для АО «Узнацбанк» и его бизнеса и технологических процессов;
- возможные угрозы информационной безопасности для объекта защиты;
- наличие уязвимостей;
- принятые меры обеспечения информационной безопасности объекта защиты.

9.21. Результат анализа рисков и угроз информационной безопасности, возникающих (могущих возникнуть) на объектах защиты приведен в Таблице №2.

9.22. Для оценки рисков использовалась следующая шкала:

- высокая – 6-8;
- средняя – 3-5;
- низкая – 0-2.

Ценность (значимость) объекта защиты для АО «Узнацбанк»

оценивалась по шкале от 0 до 10.

При данной оценки рисков информационной безопасности учитывались только актуальные угрозы.

9.23. Анализ рисков информационной безопасности возникающих (могущих возникнуть) при взаимодействии со сторонними организациями, а также при их доступе к информационным системам и ресурсам АО «Узнацбанк» и взаимодействии информационных систем (ИАБС, Система процессинга для обслуживания клиентов VISA/MasterCard-карт) АО «Узнацбанк» с информационными системами сторонних организаций, приведен в таблице №3.

9.24. Для снижения рисков информационной безопасности при взаимодействии со сторонними организациями должны реализовываться меры безопасности в отношениях с внешними пользователями, которые приведены в разделе 11 настоящей Политики.

9.25. Риски информационной безопасности регулярно оцениваются и анализируются УИБ ДИББ не менее одного раза в год, в период проведения внутреннего аудита информационной безопасности. По итогам оценки рисков определяется актуальный перечень рисков информационной безопасности, оценивающие как «высокий».

Таблица №2. Результат анализа и оценки рисков информационной безопасности в отношении объектов защиты АО «Узнацбанк»

№	Наименование актуальной угрозы	Вероятность угрозы	Последствия	Принятые меры	Оценка риска
1.	Средствам обработки и хранения информации (сервера БД и приложений и системы хранения данных) и используемое на них программное обеспечение (операционная система, СУБД, приложения и прикладные программы) **информационных систем АО «Узнацбанк»: ИАБС, БИС, Система процессинга для обслуживания клиентов VISA/MasterCard-карт** **Ценность (значимость) - 10**				
1.1	Заражение вредоносной программой	0,6	Нарушение нормального функционирования, полный выход из строя системы	Применение антивирусных средств	6 (высокая)
1.2	Отказ в обслуживании	0,8	Нарушение нормального функционирования, невыполнение отдельных технологических задач, полный выход из строя системы	Резервирование серверов, системы хранения данных и хранящейся информации	6 (высокая)
1.3	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	0,7	Нарушение нормального функционирования, полный выход из строя системы	Применение IDPS	7 (высокая)
1.4	Сетевые атаки, направленные на получение несанкционированного доступа	07	Нарушение нормального функционирования, доступ к информации (нарушение конфиденциальности или целостности, модификация) или к средствам (контроль управления, внесение изменений в настройку)	Применение IDPS и межсетевых экранов	7 (высокая)
1.5	Несанкционированный физический доступ	0,4	Нарушение нормального функционирования, доступ к информации (нарушение конфиденциальности или целостности) или к средствам	Ограничение доступа в серверные помещения ЦОД	3 (средняя)

			(контроль управления, внесение изменений в настройку)		
1.6	Техногенные угрозы и стихийные природные явления (чрезвычайные ситуации)	0,2	Потеря находящихся в помещении средств и информации (финансовые потери), нарушение функционирования	Использование резервного ЦОД	2 (низкая)
2.	Средствам обработки информации (сервера) и используемое на них программное обеспечение (операционная система, приложения и прикладные программы) **СЭД, корпоративной электронной почты** **Ценность (значимость) - 8**				
2.1	Заражение вредоносной программой	0,6	Нарушение нормального функционирования, полный выход из строя системы	Применение антивирусных средств	6 (высокая)
2.2	Отказ в обслуживании	0,8	Нарушение нормального функционирования, невыполнение отдельных технологических задач, полный выход из строя системы	Резервирование серверов и информации	7 (высокая)
2.3	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	0,7	Нарушение нормального функционирования, полный выход из строя системы	Применение IDPS	6 (высокая)
2.4	Сетевые атаки, направленные на получение несанкционированного доступа	07	Нарушение нормального функционирования, доступ к информации (нарушение конфиденциальности или целостности, модификация) или к средствам (контроль управления, внесение изменений в настройку)	Применение IDPS и межсетевых экранов	7 (высокая)
2.5	Несанкционированный физический доступ	0,4	Нарушение нормального функционирования, доступ к информации (нарушение конфиденциальности или	Ограничение доступа в серверное помещение	3 (средняя)

			целостности) или к средствам (контроль управления, внесение изменений в настройку)		
2.6	Техногенные угрозы и стихийные природные явления (чрезвычайные ситуации)	0,2	Потеря находящихся в помещении средств и информации (финансовые потери), нарушение функционирования	Задействование ресурсов резервного ЦОД	3 (средняя)
3	Сетевое оборудование (коммутаторы ядра, маршрутизаторы) и каналы связи **корпоративной сети** **Ценность (значимость) - 8**				
3.1	Отказ в обслуживании сетевого оборудования	0,6	Нарушение нормального функционирования, потеря связи на отдельном или всех направлениях	Резервирование сетевого оборудования	6 (высокая)
3.2	Отключение канала связи	0,5	Потеря связи по направлению или выхода в Интернет или взаимодействие с внешними информационными системами	Резервирование каналов связи	7 (высокая)
3.3	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	0,7	Нарушение нормального функционирования, полный выход из строя средства	Применение IDPS (исключение маршрутизаторы)	6 (высокая)
3.4	Сетевые атаки, направленные на получение несанкционированного доступа	07	Нарушение нормального функционирования, (контроль управления, внесение изменений в настройку) к средствам	Применение IDPS и межсетевых экранов, (исключение маршрутизаторы)	6 (высокая)
3.5	Несанкционированный физический доступ	0,4	Нарушение нормального функционирования, доступ к средствам (контроль управления, внесение изменений в настройку)	Ограничение доступа в серверные помещения	3 (средняя)
	Угрозы с использованием технических каналов утечки	0,3	Утечка информации, воздействие и подавление	Защищенное размещение средств	2 (низкая)

	информации		технических средств и каналов связи	и каналов, меры по проводкам	
3.6	Техногенные угрозы и стихийные природные явления (чрезвычайные ситуации)	0,2	Потеря находящихся в помещении средств (финансовые потери), нарушение функционирования	Задействование сетевого обордования резервного ЦОД	3 (средняя)
4	Сетевое оборудование (коммутаторы) и каналы связи **ЛВС головного офиса региональных и районных филиалов** **Ценность (значимость) - 5**				
4.1	Отказ в обслуживании сетевого оборудования	0,6	Нарушение нормального функционирования, потеря связи для одного или нескольких рабочих станций и серверов	Задействование резервного сетевого оборудования	5 (средняя)
4.2	Выход из строя кабеля	0,4	Потеря связи для одного или нескольких рабочих станций и серверов	Восстановление кабеля	5 (средняя)
4.3	Несанкционированный физический доступ	0,4	Нарушение нормального функционирования	Размещение в шкафах и помещениях	3 (средняя)
	Угрозы с использованием технических каналов утечки информации	0,3	Утечка информации, воздействие и подавление технических средств и каналов связи	Защищенное размещение средств и каналов, меры по проводкам	2 (низкая)
3.6	Техногенные угрозы и стихийные природные явления (чрезвычайные ситуации)	0,2	Потеря находящихся в помещении средств (финансовые потери), нарушение функционирования	Восстановление или использование резервных коммутаторов	2 (низкая)
5	**Рабочие станции сотрудников** и установленное на них программное обеспечение (операционная система и прикладное программное обеспечение) **Ценность (значимость) - 5**				
5.1	Заражение вредоносной программой	0,6	Нарушение нормального функционирования, полный выход из строя, потеря информации	Применение антивирусных средств	5 (средняя)
5.2	Отказ в обслуживании рабочей	0,6	Нарушение нормального	Профилактика,	4

	станции, его компонента или ПО		функционирования, потеря информации	резервирование информации на дисках	(средняя)
5.3	Несанкционированный физический доступ	0,4	Нарушение нормального функционирования, утечка или уничтожение информации	Установка пароля, контроль действий посетителей	5 (средняя)
5.4	Утечка информации со стороны сотрудника по каналам связи (электронная почта, мессенджеры, сотовые телефоны и т.д.)	0,8	Утечка (нарушение конфиденциальности) информации	Контроль каналов утечек информации	7 (высокая)
5.5	Угрозы с использованием технических каналов утечки информации	0,2	Утечка информации	Размещение в контролируемой зоне	1 (низкая)
5.6.	Техногенные угрозы и стихийные природные явления (чрезвычайные ситуации)	0,2	Потеря находящихся в помещении средств и информации, нарушение функционирования	Восстановление или использование резервных рабочих станций	2 (низкая)
6	**Конфиденциальная информация в бумажном виде Ценность (значимость) - 7**				
6.1	Несанкционированный физический доступ	0,5	Нарушение конфиденциальности информации	Размещение в сейфах и контроль выдачи	7 (высокая)
7	**Банкоматы, киоски, платежные терминалы и электронные платежные устройства Ценность (значимость) - 7**				
7.1	Несанкционированный физический доступ	0,5	Нарушение нормального функционирования, кража, взлом, осуществение несанкционированных действий	Размещение в помещениях с ограниченным доступом или охраной, использование системы видеонаблюдения	7 (высокая)

Таблица №3. Результат анализа и оценки рисков информационной безопасности при взаимодействии со сторонними организациями

Актуальные угрозы	Последствия	Риски
При взаимодействии со сторонними организациями, а также при их доступе к информационным системам и ресурсам АО «Узнацбанк», средствам обработки, хранения и передачи информации и программному обеспечению (физический доступ)		
Получение несанкционированного физического доступа к средствам	Нарушение их нормального функционирования, вывод из строя, установка средств съема информации или несанкционированного управления средствами	3 (средний)
Получение несанкционированного физического доступа к информации	Нарушение конфиденциальности и целостности информации	3 (средний)
В рамках взаимодействия информационных систем АО «Узнацбанк» с информационными системами сторонних организаций для обмена с ними информацией, а также с внешними пользователями информационных систем АО «Узнацбанк» при оказании интерактивный услуг		
Получение несанкционированного сетевого доступа к средствам и информации информационной системы	Нарушение нормального функционирования, вывод из строя, несанкционированное управление средствами, нарушение конфиденциальности, целостности информации, её блокирование и утрата	7 (высокий)
Распространение вредоносной программы	Нарушение нормального функционирования, потеря информации	6 (высокий)

10. Модель нарушителя информационной безопасности

10.1. Модель нарушителя формируется для систематизации данных о возможностях и типах субъектов, целях несанкционированных воздействий и выработки адекватных соответствующих методов противодействия. При разработке модели нарушителя должны учитываться:

- категории нарушителя;
- характеристики нарушителя для оценки степени опасности и важности и анализа его технической мощности.
- ограничительные меры и методы противодействия.

10.2. Нарушитель информационной безопасности - это лицо, которое предприняло попытку выполнения запрещенных операций (действий), направленных на нарушение информационной безопасности по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

10.3. Нарушителями по отношению к объектам защиты АО «Узнацбанк» могут быть его сотрудники, имеющие непосредственный допуск к объектам защиты, сотрудники, не имеющие допуск к объектам защиты, и лица, не являющиеся сотрудниками АО «Узнацбанк».

10.4. Основные группы и классы нарушителей:

10.4.1. При рассмотрении нарушителей необходимо разделить их на группы по отношению к объектам защиты и соответственно возможностям воздействия на его компоненты. Групп нарушителей две:

1) внешние нарушители– физические лица, не обладающие правами доступа внутрь контролируемой зоны и соответственно не имеющие возможности прямого воздействия на объект защиты и его компоненты;

2) внутренние нарушители – физические лица, обладающие правами доступа внутрь контролируемой зоны и соответственно имеющие доступ к объекту защиты и его компонентам.

10.4.2. Согласно среднемировой статистике 82% угроз в банках совершается собственными сотрудниками при их прямом или опосредованном участии, 17% угроз совершается извне – внешние угрозы и 1% угроз совершается случайными лицами.

Исходя из данной статистики, в отношении внутренних сотрудников АО «Узнацбанк» должны приниматься усиленные меры контроля и защиты от совершения с их стороны незаконных действий. В частности к таким мерам относятся: определение шаблон-ролевой моделей по допуску лиц к работе в информационных системах или получающих доступ к объектам защиты, учет действий сотрудников в информационных системах, разграничение доступа (предоставление определенных прав) сотрудников к информационным системам и управление этим доступом, контроль привилегированных пользователей, снижение возможных каналов утечек, осведомление сотрудников о рисках и последствиях за совершение незаконных действий и т.д.

10.4.3. Вне зависимости от групп, нарушитель может относиться к одному из четырех классов по возможным действиям:

- первый (низкий) уровень (класс 1) возможностей нарушителя характеризуется запуском задач из фиксированного набора с заранее предусмотренными функциями по обработке информации;

- второй (класс 2), включает возможности пользователей первого уровня и дополнительно имеет возможности создания и запуска собственных программ с новыми функциями по обработке информации. Таким образом, возможна ситуация, когда внешний нарушитель реализует внутренние угрозы;

- третий (класс 3), имеет возможность управления функционированием объектом защиты, то есть воздействовать на базовое программное обеспечение, его состав и конфигурацию;

- четвертый (класс 4), отличается полным объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств объектов защиты, вплоть до включения в состав объекта защиты технических и программных средств с новыми функциями по обработке данных.

10.4.4. Различение нарушителей по квалификации, как специалиста в области информационных технологий:

- неопытный пользователь (класс А): нарушитель этого класса предоставляет опасность как источник невнимательных или неверных действий на объект защиты, которые редко, но могут привести к сбою или даже отказу

работы системы, непреднамеренным действиям и нанести ущерб банку;

- уверенный пользователь (класс Б): данный класс нарушителя может быть источником нарушений работы объекта защиты, но попытки установить свои программы, воспользоваться внешними ресурсами, в том числе Интернет, будут пресечены системой разграничения доступа и средствами защиты информации;

- высококвалифицированный пользователь (класс В): все попытки нарушителя данного класса обойти установленные правила разграничения доступа и средства защиты информации должны фиксироваться системой аудита безопасности, блокироваться системой защиты.

10.5. Модели нарушителей информационной безопасности составляется и поддерживается в отношении каждого важного и критичного объекта защиты АО «Узнацбанк» и включается в модель угроз объекта защиты.

10.6. Модель нарушителей информационной безопасности для АО «Узнацбанк» включает следующих нарушителей с соответствующими категориями, характеристиками и ограничительными мерами в отношении них:

10.6.1. Внутренние нарушители:

1) Сотрудники банка, являющимися зарегистрированные (авторизованными) пользователями сетей и информационных систем АО «Узнацбанк». По возможным действиям относятся к 1 классу, а по опытности – классам А и Б.

Характеристики данного нарушителя: наличие возможности по реализации угроз, которые сводятся, в основном, к попыткам расширения своих полномочий и преодолению средств защиты информации с использованием только штатных программных и технических средств взаимодействия с объектом защиты, наличие возможности осуществления утечки защищаемой информации.

Ограничительные меры в отношении данных нарушителей: разграничение прав и управление доступом к объектам защиты, учет действий сотрудников в информационных системах, снижение и контроль каналов утечек информации, соблюдение требований по неразглашению конфиденциальной информации.

2) Сотрудники банка, не являющиеся пользователями информационных систем и сетей (охрана, технический персонал, обслуживающий здание и помещение и др.). По возможным действиям могут относиться к 1 классу и по опытности – классу А.

Возможности по реализации угроз данного вида внутреннего нарушителя сводятся к получению несанкционированного физического доступа к объекту защиты и в основном выступают как источник невнимательных или неверных действий на объект защиты, которые могут привести к сбою или даже отказу работы системы.

Ограничительные меры в отношении данных нарушителей: выполнение требований по размещению объектов защиты, использование в отношении объекта комплекса режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированного

физического доступа и действий, подбор и расстановка кадров, предоставление и управление допуском в помещение, в которых расположены объекты защиты.

3) Персонал, обслуживающий технические средства АО «Узнацбанк». По возможным действиям относятся к 3 классу и по опытности – классу В.

Характеристики данного нарушителя: наличие санкционированного доступа к техническим и программным средствам объекта защиты, но не являясь их зарегистрированным пользователем. Возможности данного вида нарушителя существенным образом зависят от действующих ограничительных факторов по допуску физических лиц в помещения, в которых расположен объект защиты, и контролю за порядком проведения работ.

4) Администраторы, обслуживающие сети, информационные системы и средства защиты информации АО «Узнацбанк». По возможным действиям относятся к 4 классу и по опытности – классам Б и В.

Характеристики данного нарушителя: наличие санкционированного доступа к объекту защиты и являются членами группы привилегированных пользователей. Особенность нарушителя данного вида состоит в том, что они входят в число доверенного персонала объекта защиты и им предоставляются широкие возможности для реализации угрозы по воздействию на внутреннее состояние компонентов объекта защиты.

Ограничительные меры в отношении данных нарушителей: учет и контроль действий данных сотрудников при обращении к объекту защиты.

5) Специалисты, являющиеся разработчиками информационных систем АО «Узнацбанк». По возможным действиям относятся к 1 классу, а по опытности – к классам А и Б.

Характеристики данного нарушителя: наличие возможности по реализации угроз, которые сводятся к ошибкам разработчиков при разработке прикладной программы информационной системы или установке недекларированных функциональных возможностей (закладок) для совершения в дальнейшем противоправных действий, связанных с нарушением нормального функционирования прикладной программы или утечки информации.

Ограничительные меры в отношении данных нарушителей: учет и контроль действий данных сотрудников при разработке, осуществление анализа разработанных программ отдельными сотрудниками АО «Узнацбанк» с применением анализаторов исходного кода, тестирование функциональных возможностей, входных и выходных данных программы сторонними сотрудниками АО «Узнацбанк».

10.6.2. Внешние нарушители:

1) Уволенные сотрудники АО «Узнацбанк». По возможным действиям и опытности относятся к классу в зависимости от ранее занимаемой им должности (бывший пользователь или не являвшийся пользователем сетей и информационных систем, или технический обслуживающий персонал, или администратор).

Характеристики данного нарушителя: возможности по реализации угроз данного вида внешнего нарушителя сводятся к раскрытию или использованию

защищаемой информации АО «Узнацбанк», в том числе технологической и технической по получению несанкционированного доступа и обходу средств защиты информации, с целью получения личной выгоды, нанесения ущерба бывшей организации, совершения противоправных действий.

Ограничительные меры в отношении данных нарушителей: выполнение обязательств по неразглашению конфиденциальной информации как уволенный сотрудник, исключение возможности использования их реквизитов доступа после увольнения.

2) Посетители, являющиеся клиентами банка.

Характеристики данного нарушителя: возможности по реализации угроз данного вида внешнего нарушителя сводятся к получению несанкционированного физического доступа к объекту защиты.

Ограничительные меры в отношении данных нарушителей: выполнение требований по размещению объектов защиты, ограничение доступа посетителей в неразрешенные для них помещения (зоны) с применением комплекса режимных и организационно-технических мер.

3) Посетители, являющиеся представителями сторонних организаций, выполняющих какие-либо работы (поставщики услуг) в АО «Узнацбанк». По возможным действиям могут относится ко 2-4 классу и по опытности – классам Б и В.

Характеристики данного нарушителя: наличие санкционированного доступа к объекту защиты, но не являясь их зарегистрированным пользователем – разработчики аппаратных и программных средств объекта защиты, осуществляющие их установку, пуско-наладочные работы, сопровождение в период эксплуатации и т.д.. Особенность данного вида нарушителя в том, что он может осуществлять различные действия в зависимости от алгоритма функционирования, заложенного в специальных деструктивных средствах. Активизация специальных деструктивных средств может произойти в любой момент работы объекта защиты на протяжении всего его жизненного цикла.

Ограничительные меры в отношении данных нарушителей: контроль порядка проведения работ, присутствие представителя АО «Узнацбанк» при проведении этих работ, предоставление доступа только к требуемым средствам объекта защиты, контроль за этим доступом, соблюдение технических требований при проектировании продукта, тестирование на уязвимости по принципу «белых хакеров».

4) Нарушители, получившие несанкционированный доступ к объекту защиты из вне через внешнюю сеть, обойдя систему защиты. По квалификации данный нарушитель относится к классу В, а по возможным действиям может относится к 2 и 3 классу.

Характеристики данного нарушителя: совершение целенаправленных действий путем применения специальных программно-технических средств или уязвимостей в системе.

Ограничительные меры в отношении данных нарушителей: применение комплекса аппаратно-программных средств защиты, направленных на

предотвращение и пресечение несанкционированных действий данных нарушителей.

XI. Меры информационной безопасности

11.1. Для построения СУИБ в АО «Узнацбанк» должны реализовываться все меры обеспечения информационной безопасности, которые подразделяются на:

- правовые меры;
- морально-этические меры;
- организационные меры;
- технологические меры;
- инженерно-технические меры;
- программно-аппаратные меры;
- меры безопасности в отношениях с внешними пользователями.

11.1.1. **Правовые меры**

К правовым мерам защиты относятся действующие в стране нормативные акты, регламентирующие вопросы обеспечения информационной безопасности, а также внутренние нормативные документы АО «Узнацбанк».

Правовые меры реализуются путем проведения соответствующих мероприятий, связанных с формированием комплекса нормативных и организационно-распорядительных документов (правила, регламенты, порядки, положения, требования, инструкции, методики, руководства, обязанности, перечни, планы, мероприятия, формуляры и т.п.), регламентирующих вопросы обеспечения информационной безопасности в АО «Узнацбанк» в целом и на отдельных объектах защиты в частности.

Нормативная база АО «Узнацбанк» в области обеспечения информационной безопасности должна формироваться в виде трехуровневой системы нормативных и организационно-распорядительных документов, которыми должны руководствоваться сотрудники АО «Узнацбанк».

Документом первого уровня является настоящая Политика информационной безопасности.

В перечень документов второго уровня входят документы:

- определяющие перечень критичных и важных ресурсов защиты, их категорию и класс защищенности, включая перечень конфиденциальной информации;
- организационного и распорядительного порядка, направленные на реализацию мер по обеспечению информационной безопасности и распределения обязанностей и ответственности среди сотрудников;
- устанавливающие порядок и регламентирующие процессы и процедуры обеспечения информационной безопасности.

Перечень документов третьего уровня включает рабочие формы, журналы, отчеты, заявки, протоколы и другие документы, используемые для регистрации и подтверждения выполненных процедур и работ по обеспечению информационной безопасности.

Отдельные документы второго и третьего уровня приведены в приложениях к настоящей Политики.

Разработку внутренних нормативных документов по обеспечению информационной безопасности в АО «Узнацбанк» осуществляет ДИББ. Также этим подразделением вносятся предложения и принимаются меры по совершенствованию нормативной базы АО «Узнацбанк» в области обеспечения информационной безопасности.

Внутренние документы по информационной безопасности и изложенные в них требования должны быть доведены до каждого сотрудника АО «Узнацбанк» и строго соблюдаться этими сотрудниками.

11.1.2. **Морально-этические (психологические) меры защиты информации**

Морально-этические (психологические) меры защиты информации направлены на:

- создание здорового морального климата в коллективе;
- снижение вероятности возникновения негативных действий и нарушений информационной безопасности, связанных с человеческим фактором;
- исключение личностных психологических факторов при нарушении режима защиты информации;
- соблюдение сотрудниками АО «Узнацбанк» правил этического поведения.

Морально-этические меры защиты являются профилактическими, к которым относятся:

- проведение разъяснительных работ среди сотрудников АО «Узнацбанк»;
- психологический мониторинг;
- применение дисциплинарных мер в отношении нарушителей;
- побуждение и поощрение сотрудников.

Разъяснительные работы проводятся ДИББ АО «Узнацбанк» среди сотрудников АО «Узнацбанк» в виде специальных занятий или индивидуальных бесед.

Данная разъяснительная работа направлена на:

- повышение уровня знаний сотрудников АО «Узнацбанк» касательно влияния угроз на деятельность АО «Узнацбанк» и о возможных последствиях, а также о мерах ответственности, которые могут быть применены в отношении нарушителей;
- выработку сознания у сотрудников АО «Узнацбанк» в необходимости выполнения элементарных процедур и требований настоящей Политики информационной безопасности;
- повышение степени сознательности и ответственности сотрудников в вопросах обеспечения информационной безопасности;
- выработку требуемых норм поведения и нравственности, которые способствуют соблюдению правил и требований обеспечения информационной безопасности;

- создание сплоченности сотрудников при решении задач обеспечения информационной безопасности.

Разъяснительные работы проводятся не реже одного раза в год отдельно для следующих групп сотрудников АО «Узнацбанк»:

- работники АО «Узнацбанк», не взаимодействующих непосредственно с клиентами банка;
- работники АО «Узнацбанк», взаимодействующие с клиентами банка;
- работники АО «Узнацбанк», обеспечивающие обслуживание информационных систем и ресурсов, технического и технологического оборудования банковской информационной инфраструктуры АО «Узнацбанк».

В отношении новых сотрудников АО «Узнацбанк» должен проводиться вводный инструктаж по вопросам обеспечения информационной безопасности.

Психологический мониторинг применяется как к отдельной личности, так и к подразделения и АО «Узнацбанк» в целом, что позволяет быстро выявить какие-либо волнения среди сотрудников, определять ответственных и добросовестных сотрудников в отношении соблюдения правил и норм, так и безответственных и халатных сотрудников, которых следует взять на контроль и принять в отношении них соответствующие меры.

Дисциплинарного правового меры должны быть направлены для создания условий, при которых сотрудники АО «Узнацбанк» будут вынуждены соблюдать правила и требования по обеспечению информационной безопасности, а именно меры наказания на случай их нарушения.

В отношении нарушителей руководством АО «Узнацбанк» могут применяться меры дисциплинарного взыскания в соответствии с трудовым законодательством в рамках трудовых договоров и контрактов.

Меры побуждения должны быть направлены для создания условий, которые мотивируют сотрудников АО «Узнацбанк» к должному поведению. К данным мерам относятся поощрительные меры.

В отношении отличившихся сотрудников, надлежаще выполняющих трудовые обязательства, должны приниматься поощрительные меры в виде объявления благодарности, предоставления почетных грамот, денежной премии или ценного подарка, а за особые услуги представлены к государственным наградам в порядке, установленном законодательством.

В целях предупреждение правонарушений, устранение причин и условий, способствующих их совершению, со стороны всех сотрудников АО «Узнацбанк» должны соблюдаться Типовые правила этического поведения работников органов государственного управления и органов исполнительной власти на местах, утвержденные постановлением Кабинета Министров от 2 марта 2016г. № 62.

11.1.3. **Организационные меры**

Организационные меры в АО «Узнацбанк» направлены на:

- распределение обязанностей и ответственности между подразделениями и сотрудниками;
- определение и классификацию объектов защиты, анализ и оценку рисков информационной безопасности;

- защиту и неразглашение конфиденциальной информации;

- создание, функционирование и развитие системы и средств защиты информации;

- реагирование на инциденты информационной безопасности;

- повышение уровня квалификации и осведомленности сотрудников в области обеспечения информационной безопасности;

- оценку уровня защищенности;

- обеспечение физической защиты.

1) В части распределения обязанностей и ответственности между подразделениями и сотрудниками АО «Узнацбанк» принимаются следующие организационные меры:

а) определение лица из числа руководителей правления АО «Узнацбанк», курирующего вопросами обеспечения информационной безопасности в АО «Узнацбанк»;

б) распределение обязанностей между подразделениями головного офиса, региональных и районных филиалов в части обеспечения информационной безопасности;

в) назначение ответственных лиц по информационной безопасности в головном офисе, региональных и районных филиалах АО «Узнацбанк» (далее - администраторы информационной безопасности), системного администратора ЛВС АО «Узнацбанк» и сетевого администратора корпоративной сети;

г) определение списка лиц, получающие как физический, так и логический доступ к объектам защиты, в том числе к конфиденциальной информации, ЦОД, коммутационными иным помещениям, ЛВС, корпоративной сети, ИАБС и иным информационным системам и ресурсам, сетевому оборудованию и средствам защиты информации;

д) определение лиц, ответственных за функционирование и эксплуатацию конкретных средств обработки, хранения, передачи информации и средств защиты информации;

е) закрепление соответствующими организационно-распорядительными документами учетных съемных носителей и накопителей данных за сотрудниками АО «Узнацбанк»;

ж) осуществление со стороны ДИББ контроля за выполнением ответственными лицами, закрепленных за ними обязанностей в части обеспечения информационной безопасности;

з) организация электронных курсов и проведение тестов в электронном виде для повышения уровня подготовки ответственных лиц, знания ими норм и обязанностей по информационной безопасности.

Распределение обязанностей между подразделениями и сотрудниками, ответственными за обеспечение информационной безопасности должно осуществляться в соответствии с Положением о ДИББ, подразделениях и сотрудниках, ответственных за обеспечение информационной безопасности, приведенным в приложении №5 к настоящей Политике, а также в соответствии с разделом 14 настоящей Политики.

2) В части определения и классификации объектов защиты, анализа и

оценки рисков информационной безопасности принимаются следующие организационные меры:

а) проведение инвентаризации для определения объектов защиты и информационных активов;

б) формирование списка объектов защиты и реестра информационных активов (ресурсов) АО «Узнацбанк», их категорирование и определение класса защищенности;

в) классификация объектов защиты по уровню защищенности в соответствии с государственным стандартом O‘ZDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;

г) определение модели угроз для каждого важного и критичного объекта защиты и проведение анализа и оценки рисков информационной безопасности в соответствии с разделом 9 настоящей Политики;

д) мониторинг банкоматов, киосков, платежных терминалов и их доступности, организация видеонаблюдения и средств защиты в виде антискимминговых устройств, оперативная передача сигналов о несанкционированном доступе в центр мониторинга, датчиков наклона и т.д.

Инвентаризация, классификация, маркировка и формирование реестра информационных активов (ресурсов) должна проводиться в соответствии с Порядком управления информационными активами, приведенным в приложении №13 к настоящей Политике.

Инвентаризация для определения объектов защиты и информационных активов организуется и проводится Управлением информационной безопасности (УИБ) ДИББ не реже одного раза в год. По итогам инвентаризации при необходимости вносятся изменения и дополнения в список объектов защиты, в реестр информационных активов (ресурсов) и перечень конфиденциальной информации АО «Узнацбанк». Дополнительно по результатам инвентаризации определяется перечень помещений, состав входящих в них комплекса технических и программных средств.

Категорирование и классификация объектов защиты осуществляется в соответствии с O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации» и требованиями иных нормативных документов.

3) В части защиты и неразглашения конфиденциальной информации принимаются следующие организационные меры:

а) внесение изменений и дополнений в перечень защищаемой конфиденциальной информации АО «Узнацбанк»;

б) определение и утверждение списка лиц, допущенных к информации, входящей в перечень конфиденциальной информации;

в) определение в трудовых договорах требований и ответственности за неразглашение конфиденциальной информации при приеме сотрудников на работу и ознакомление их под роспись с перечнем конфиденциальной информации и мерами ответственности.

Перечень защищаемой конфиденциальной информации определен в приложении №1 к Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан». В данной Инструкции определены порядок формирования перечня конфиденциальной информации, порядок доступа к ней сотрудников банка, порядок работы с конфиденциальной информацией, требования к помещениям, где обрабатывается конфиденциальная информация, и ответственность за нарушение режима работы с конфиденциальной информацией.

Для сотрудников, допущенных к конфиденциальной информации, их обязательства по сохранности конфиденциальной информации и ответственность определяются в Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

4) В части создания, функционирования и развития системы и средств защиты информации принимаются следующие организационные меры:

а) закупка средств защиты информации в рамках реализации мероприятий по обеспечению информационной безопасности АО «Узнацбанк»;

б) определение технических требований к закупаемым средствам защиты информации;

в) проведение организационных мероприятий по подготовке к внедрению и обеспечению эксплуатации системы и средств защиты информации, к которым относятся выделение помещения, разработка инструкций по эксплуатации, закрепление ответственного сотрудника и прохождение им обучения по эксплуатации;

г) проведение опытно-эксплуатационных и приемно-сдаточных испытаний при внедрении средств защиты информации;

д) осуществление управления (администрирования) системой защиты, включающий в себя контроль конфигурации и параметров настройки, восстановление работоспособности, установку обновлений программного обеспечения, корректировку эксплуатационной документации, контроль за событиями безопасности, документирование процедур и результатов контроля;

е) подготовка и внесение предложений по совершенствованию системы защиты информации в случае выявления недостатков в функционировании и обеспечении защищенности.

5) В части выявления, ликвидации последствий и проведения расследований по инцидентам информационной безопасности принимаются организационные меры, которые определены в разделе 12 настоящей Политики.

6) В части повышения уровня квалификации и осведомленности сотрудников в области обеспечения информационной безопасности принимаются следующие организационные меры:

а) прохождение переподготовки и повышения квалификации сотрудниками АО «Узнацбанк», ответственными за обеспечение информационной безопасности, на регулярной основе;

б) организация и проведение обучения сотрудников АО «Узнацбанк» с целью повышения их осведомленности и выполнение ими требований и положений настоящей Политики;

в) проведение аттестации сотрудников АО «Узнацбанк» по итогам обучения для проверки уровня их осведомленности;

г) ознакомление каждого сотрудника АО «Узнацбанк» с настоящей Политикой информационной безопасности под роспись в журнале, форма которой приведена в приложении №19, и касающихся их внутренних нормативных документов по обеспечению информационной безопасности.

Для повышения квалификации сотрудников, ответственных за обеспечение информационной безопасности, а также обучения сотрудников АО «Узнацбанк» по вопросам защиты информации УИБ ДИББ ежегодно составляется и утверждается график курсов повышения квалификации специалистов, проведения тренингов и семинаров для сотрудников АО «Узнацбанк».

7) В части оценки уровня защищенности принимаются следующие организационные меры:

а) проведение внутреннего и внешнего аудита для оценки уровня защищенности объектов защиты и актуализации настоящей Политики;

б) организация проведения аттестации объектов информатизации АО «Узнацбанк» аккредитованными организациями согласно постановлению Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572«О дополнительных мерах по защите национальных информационных ресурсов»;

в) проведение экспертизы официального веб-сайта АО «Узнацбанк» на соответствие требованиям информационной безопасности;

г) проведение оценки эффективности принятых организационных, технических и иных мер защиты, а также устранение выявленных недостатков по итогам аудитов, экспертиз и аттестаций.

Регулярность проведения внутреннего аудита должна составлять не менее 1 раза в год, а внешнего аудита – не менее 1 раза в три года.

Внутренний аудит проводится подразделениями ДИББ. Для проведения внешнего аудита информационной безопасности привлекаются сторонние организации, компетентные проводить такой аудит.

8) В части обеспечения физической защиты принимаются следующие организационные меры:

а) организация охраны и пропускного режима при входе на территорию и в здание головного офиса, региональных и районных филиалов, мини банков;

б) разделение помещений зданий головного офиса, региональных и районных филиалов, мини банков на зоны доступа;

в) прием и обслуживание клиентов и посетителей банка в операционных залах и комнатах приема (первая-зона);

г) размещение объектов информатизации на максимально возможном

расстоянии относительно границы контролируемой зоны, а их технические средства обработки информации, передачи и защиты информации - в защищаемых серверных помещениях ЦОД и коммутационных помещениях;

д) хранение документированной конфиденциальной информации и съемных носителей конфиденциальной информации в сейфах, шкафах или иных защищенных хранилищах, учет носителей конфиденциальной информации.

Организация охраны объектов АО «Узнацбанк» осуществляется в соответствии с требованиями постановления Министерства внутренних дел и Правления Центрального банка Республики Узбекистан от 5 июня 2010 года №12, 22/7-ДСП «Об утверждении инструкции об организации охраны банков и их филиалов подразделениями охраны при органах внутренних дел Республики Узбекистан».

В соответствии с Типовым порядком организации допуска в филиалах акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан» (рег. №509/19 от 17.03.2020 г.) помещений делятся на следующие зоны:

1-зона – помещения банка, вход в которые не ограничен для сотрудников банка и клиентов (информационный зал, операционный зал, кредитный отдел и др.);

2-зона - помещения банка, вход в которые разрешен должностным лицам, являющимся сотрудниками АО «Узнацбанк» (операционное отделение, кассовые помещения, помещения подразделений);

3 зона - помещения банка, вход в которые разрешён строго определённым должностным лицам, являющимся сотрудниками АО «Узнацбанк» (денежные хранилища, помещения с секретными документами, помещения хранения оружия и боеприпасов службы инкассации, помещения в ЦОД и др.) и контролируется соответствующими средствами контроля доступа.

11.1.4. **Технологические (технические) меры**

Технологические (технические) меры обеспечения информационной безопасности АО «Узнацбанк» направлены на:

- обеспечение пожарной безопасности и климатических условий для нормального функционирования средств обработки, хранения и передачи информации;
- резервирование технических средств обработки, хранения, передачи и защиты информации;
- резервирование каналов связи;
- резервирование информации и информационных ресурсов;
- обеспечение гарантированного электропитания;
- обеспечение информационной безопасности при выводе из эксплуатации объектов защиты.

В основных помещениях зданий головного офиса АО «Узнацбанк», а также в коммутационных помещениях региональных и районных филиалов установлены системы пожарной сигнализации. В серверных помещениях основного и резервного ЦОД АО «Узнацбанк» используется автоматическая

система пожаротушения.

В основном и резервном ЦОД АО «Узнацбанк», коммутационных помещениях региональных и районных филиалов применяются средства обеспечения требуемых климатических условий (кондиционеры).

По обеспечению нормального функционирования основного и резервного ЦОД, они должны отвечать требованиям O'zDSt 2875:2014 «Требования к дата-центрам. Обеспечение инфраструктуры и информационной безопасности».

Резервированию подлежат следующие технические средства АО «Узнацбанк»:

- сервера (базы данных и веб-приложений) и система хранения данных информационных систем АО «Узнацбанк»;
- маршрутизаторы, используемые для подключения основного ЦОД и головного офиса к внешней и корпоративной сети;
- коммутаторы ядра сети;
- межсетевой экран и средства обнаружения и предотвращения вторжений (IDPS), используемые на границе подключения основного ЦОД и головного офиса к внешней сети.

Резервированию подлежат каналы связи, используемые для подключения головного офиса (основного ЦОД) и резервного ЦОД к внешней сети и корпоративной сети.

Требования по резервированию средств обработки, хранения, передачи и защиты информации, а также каналов связи определены в Плане обеспечения непрерывной работы и восстановления работоспособности в чрезвычайных (аварийных) ситуациях, приведенном в приложении №17 к настоящей Политике.

Резервному копированию подлежит база данных и журналы (логи) информационных систем АО «Узнацбанк», а также конфигурируемые параметры (настройки) сетевого оборудования и средств защиты информации. Резервное копирование и восстановление данных в АО «Узнацбанк» осуществляется в соответствии с Положением по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных, приведенным в приложении №6 к настоящей Политике.

Для обеспечения резервирования данных используются системы резервирования и восстановления данных, указанные в Положении по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных, приведенном в приложении №6 к настоящей Политике.

В целях обеспечения бесперебойного электропитания АО «Узнацбанк» предусмотрены следующие меры:

- установка дизель-генератора и источников бесперебойного питания для бесперебойного питания серверного и сетевого оборудования и средств защиты информации в здании головного офиса (основной ЦОД) и отдельно в здании резервного ЦОД;

- использование дополнительных источников бесперебойного питания UPS для серверов, сетевого оборудования, средств защиты информации, которые установлены в основном и резервном ЦОД, коммутационных помещениях региональных и районных филиалах.

В целях обеспечения информационной безопасности при выводе из эксплуатации объектов защиты или после принятия решения об окончании обработки информации должны выполняться меры по уничтожению (стирание) данных и остаточной информации с носителей информации и (или) физическому уничтожению носителей информации.

Уничтожение (стирание) данных и остаточной информации с носителей информации и (или) физическое уничтожение носителей информации при выводе их из эксплуатации осуществляется в соответствии с Инструкцией по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных, приведенной в приложении №9 к настоящей Политике.

Документированная конфиденциальная информация подлежит уничтожению с применением специального уничтожителя (шредер).

11.1.5. **Инженерно-технические меры**

Инженерно-технические меры направлены на предотвращение физического доступа или создания препятствий для проникновения посторонних физических лиц к объектам защиты и включают следующие меры:

1) применение на входе в здание головного офиса, региональных и районных филиалах системы контроля доступа сотрудников (СКУД);

2) разграничение доступа между 1-зоной и зона 2 и 3 дверями и иными инженерными средствами;

3) установка на входе защищаемых помещений 2-зоны и на входе в помещения 3-зоны замков с использованием идентификационных магнитных карт сотрудников, имеющих право доступа к этим помещениям;

4) оснащение окон помещений средствами защиты от визуального наблюдения (занавески, жалюзи);

5) применение системы видеонаблюдения в основном и резервном ЦОД, а также для видеоконтроля за периметром зданий, входом в здания, коридорами зданий головного офиса, региональных и районных филиалов;

6) установка охранной сигнализация в защищаемых помещениях (помещение основного и резервного ЦОД, помещения 3-зоны и др.);

7) использование запираемых железных несгораемых шкафов для хранение документированной конфиденциальной информации и съемных носителей конфиденциальной информации;

8) опечатывание корпусов рабочих станций, серверов, сетевого оборудования и средств защиты информации для блокировки физического доступа к ним;

9) установка серверов, сетевого оборудования и средств защиты информации в специальных стойках (коммутационных шкафах), которые запираются механическим замком;

10) прокладка сетевых кабелей в защищенных местах внутри зданий и вне их в соответствии с требованиями раздела 13 настоящей Политики.

11.1.6. **Программно-аппаратные меры**

Программно-аппаратные меры обеспечения информационной безопасности АО «Узнацбанк» направлены на:

- организацию технической защиты информации;
- организацию криптографической защиты информации.

Для обеспечения технической защиты информации применяются следующие средства технической защиты информации:

- межсетевые экраны;
- средства IDPS;
- средства антивирусной защиты информации;
- средства разграничение доступа к сети, информационным системам и ресурса;
- средства контроля и анализа защищенности, а также мониторинга и управления инцидентами информационной безопасности и др.

Используемые методы и средства технической защиты информации в АО «Узнацбанк» приведены в Инструкции по организации технической защиты информации согласно приложению №14 к настоящей Политике.

Обеспечение безопасности сетевой инфраструктуры и применение межсетевых экранов осуществляется в соответствии с Положением по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, приведенным в приложении №2 к настоящей Политике.

В АО «Узнацбанк» применяются следующие аппаратно-программные межсетевые экраны и средства IDPS: CheckPoint 4800, Cisco FirePower 4110, Cisco FirePower 2120.

Межсетевые экраны и ссредства IDPS устанавливаются на границе подключения:

- корпоративной сети к сети Интернет (TAS-IX) и МСПД;
- DMZ основного ЦОД к ЛВС головного офиса и корпоративной сети;
- DMZ резервного ЦОД к корпоративной сети;
- резервного ЦОД (системы процессинга VISA/MasterCard АО «Узнацбанк») к внешней сети.

Для защиты от вредоносных программ принимаются технические меры и средства в соответствии с Инструкцией по антивирусной защите, приведенной в приложении №8 к настоящей Политике.

В качестве средств антивирусной защиты в АО «Узнацбанк» используется централизованная антивирусная система ESET Protect.

Для разграничения доступа к информационным ресурсам и система АО «Узнацбанк» разрабатывается матрица доступа в соответствии с Правилами по разработке матрицы доступа к информационным ресурсам, приведенными в приложении №10 к настоящей Политике.

Аутентификация пользователей при доступе к объектам защиты осуществляется по паролям и иным идентификаторам, которые формируются и

используются в соответствии с Инструкцией по парольной защите и аутентификации, приведенной в приложении №7 к настоящей Политике.

В качестве средств контроля и анализа защищенности, а также мониторинга и управления инцидентами информационной безопасности в АО «Узнацбанк» используются:

- для мониторинга состояния функционирования корпоративной сети, основных серверов и сетевого оборудования - программное обеспечение Zabbix;

- выявления (мониторинга) и управления инцидентами информационной безопасности в АО «Узнацбанк»– IBM QRadar SIEM;

- система анализа и контроля защищенности в АО «Узнацбанк» - MaxPatrol 8.

Криптографическая защита информации в АО «Узнацбанк» организуется с применением средств криптографической защиты информации (СКЗИ). В АО «Узнацбанк» СКЗИ используются для формирования и проверки ЭЦП для обеспечения авторства и целостности информации, а также аутентификации сотрудников и клиентов банка при доступе к информационным системам АО «Узнацбанк», а также для криптографического шифрования передаваемой ими информации. Для применения ЭЦП используются сертификаты закрытых и открытых ключей ЭЦП, изготавливаемых Центром регистрации ЭЦП АО «Узнацбанк».

В АО «Узнацбанк» должны использоваться СКЗИ, прошедшие сертификацию в органе по сертификации СКЗИ в соответствии с постановлением Президента Республики Узбекистан от 3 апреля 2007 года №ПП-614.

Используемые методы и СКЗИ в АО «Узнацбанк» приведены в Инструкции по организации криптографической защиты информации согласно приложению №15 к настоящей Политике.

11.1.7. **Меры безопасности в отношениях с внешними пользователями**

Меры безопасности в отношениях с внешними пользователями направлены на:

- исключение несанкционированного физического доступа внешних пользователей к объектам защиты АО «Узнацбанк» и его средствам;

- исключение несанкционированного сетевого доступа и обеспечение защищенного обмена информации при подключении внешних пользователей к ИАБС при оказании интерактивных банковских услуг (Интернет-банкинг и мобильный банкинг), а также при взаимодействии ИАБС и системы процессинга для обслуживания клиентов VISA/MasterCard-карт с иными информационными система сторонних организаций.

К мерам безопасности в отношениях с внешними пользователями (клиенты банка, посетители сторонних организаций, бывшие сотрудники) относятся:

1) обслуживание клиентов банка только в помещениях 1-зоны (информационные залы, операционные залы, отделы кредитования и др.) и

исключение возможности их доступа во внутренние служебные помещения АО «Узнацбанк»;

2) соблюдение режима доступа с выписыванием разовых и не разовых пропусков для посетителей сторонних организаций и бывших сотрудников банка в АО «Узнацбанк»;

3) регистрация всех посещений посторонними лицами с указанием причин и мест посещения, даты и времени входа и выхода;

4) сопровождение посетителей внутри здания сотрудниками банка;

5) ограничение доступа бывших сотрудников банка в защищаемые помещения 2-зоны и в 3-зону;

6) оснащение всех точек входа и выхода по периметру безопасности охранной сигнализацией и средствами видеонаблюдения;

7) определение требований по нераспространению конфиденциальной информации третьим лицам в договорах со сторонними организациями, осуществляющими разработку, обслуживание или поставку программного обеспечения и оборудования (поставщики услуг) для АО «Узнацбанк»;

8) контроль выполнения работ сотрудниками сторонних организаций, являющихся поставщиками услуг, на объектах защиты АО «Узнацбанк».

При обеспечении доступа сотрудников сторонних организаций, являющихся поставщиками услуг, к объектам защиты АО «Узнацбанк» на основании заключенных с ними договоров, в данных договорах или в отдельных заключаемых с ними соглашениях должен быть определен перечень конфиденциальной информации, а также условия и требования по её нераспространению третьим лицам. Также со стороны сторонней организации должны быть определены конкретные лица, которые будут получать доступ к объектам защиты и такой доступ должен предоставляться только этим лицам.

Лица от сторонних организаций, допущенных к объектам защиты АО «Узнацбанк», должны находиться и выполнять работы в присутствии сотрудника АО «Узнацбанк». Перечень работ, которые должны быть выполнены поставщиком услуг, а также порядок доступа их представителей к объектам защиты АО «Узнацбанк» должны определяться в заключаемых с ними договорах и соглашениях.

Посетителям АО «Узнацбанк» запрещается предоставлять право работать на рабочих станциях, подключенных к ЛВС и корпоративной сети АО «Узнацбанк», а также подключать их к внутренней ЛВС, если это не требуется для выполнения с их стороны обязанностей, определенных в договорах и соглашениях.

К мерам безопасности в отношениях с внешними пользователями для обеспечения защищенного обмена информации и исключения несанкционированного сетевого доступа при оказании интерактивных услуг относятся:

1) организация защищенных соединений между пользователями и ИАБС в соответствии с требованиями Положения о корпоративной сети и организации защищенных сетевых соединений, приведенного в приложении №1 к настоящей Политике;

2) реализация мер межсетевого экранирования в соответствии с Положением по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, приведенным в приложении №2 к настоящей Политике;

3) использование внешними пользователями реквизитов доступа (логин, пароль, ЭЦП) при доступе к интерактивным услугам в соответствии с Инструкцией по парольной защите и аутентификации, приведенной в приложении №7 к настоящей Политике;

4) обеспечение доступа только к определенным ресурсам ИАБС (сервисам) в соответствии с Матрицей доступа к основным информационным ресурсам АО «Узнацбанк», которая приведена в приложении №10 к настоящей Политике.

В договорах на оказание услуг, заключаемых с внешними пользователями (физические и юридические клиенты банка) должны оговариваться требования по исключению противоправных действий с их стороны при пользовании интерактивными банковскими услугами АО «Узнацбанк», обеспечению сохранности ими своих реквизитов доступа, а также разграничение ответственности сторон.

При взаимодействии ИАБС и системы процессинга VISA/MasterCard-карт со сторонними информационными системами (Anor, NIBBD, SWIFT, международная система VISA/MasterCard) обеспечиваются следующие меры:

1) ИАБС АО «Узнацбанк» интегрируется с информационными системами сторонних организаций через сервер приложений (агент API), обеспечивающие взаимодействие программных комплексов систем и обмен данным между ними;

2) подключение ИАБС к системам Anor и NIBBD осуществляется по сети передачи данных ГЦИ Центрального банка Республики Узбекистан, а к международной системе SWIFT по отдельному международному каналу передачи данных;

3) подключение системы процессинга VISA/MasterCard-карт АО «Узнацбанк» по отдельному международному каналу передачи данных;

4) обмен информацией с информационными системами Центрального банка осуществляется в шифрованном виде;

4) подключение к внешним каналам для взаимодействия с информационными системами сторонних организаций осуществляется через межсетевые экраны.

Обеспечение вышеуказанных требований прописываются в соглашениях со сторонними организациями.

XII. Реагирование на инциденты информационной безопасности

12.1. Одним из важных процессов в комплексной СУИБ АО «Узнацбанк» является процесс управления инцидентами информационной безопасности.

12.2. Основными целями процесса управления инцидентами информационной безопасности являются минимизация потерь АО «Узнацбанк», вызванных инцидентами информационной безопасности, и

снижение риска возникновения повторных инцидентов.

12.3. Основными процессами управления инцидентами информационной безопасности являются:

- быстрое обнаружение инцидентов информационной безопасности;
- анализ данных о событиях информационной безопасности;
- регистрация инцидента информационной безопасности;
- реагирование на инциденты информационной безопасности и информирование о них руководство и при необходимости заинтересованные внешние организации (Центральный банк, ГУП «Центр кибербезопасности»);
- установление источников и причин возникновения инцидентов, а также оценка их последствий;
- получение достоверной и полной информации о нарушениях информационной безопасности в АО «Узнацбанк» после обнаружения инцидента, оценка его последствий;
- минимизация нарушений работы и повреждения данных информационных систем АО «Узнацбанк», восстановление в кратчайшие сроки работоспособности информационных систем, ЛВС, корпоративной сети и информационных ресурсов при их нарушении функционирования в результате инцидента информационной безопасности;
- анализ результатов устранения последствий инцидента информационной безопасности;
- проведение расследований по инцидентам информационной безопасности, обеспечение сохранности и целостности доказательств возникновения инцидента информационной безопасности, создание условий для накопления и хранения точной информации об имевших место инцидентах информационной безопасности;
- выработка рекомендаций и реализация мер по недопущению повторного возникновения инцидентов информационной безопасности;

12.4. В целях выявления, ликвидации последствий и проведения расследований по инцидентам информационной безопасности должны проводиться следующие организационные и технические меры:

- определение лиц в подразделениях по обеспечению информационной безопасности, ответственных за выявление инцидентов и реагирование на них;
- использование системы управления инцидентами информационной безопасности (SIEM) для идентификации и управления инцидентами информационной безопасности в АО «Узнацбанк»;
- ведение журнала учета инцидентов информационной безопасности важных и критичных объектов защиты;
- организация для каждого важного и критичного объекта защиты группы реагирования из специалистов подразделений информационной безопасности, информационных технологий и иных заинтересованных подразделений для реагирования и проведения расследований по инцидентам информационной безопасности;
- обучение персонала АО «Узнацбанк» действиям по обнаружению, устранению последствий и предотвращению инцидентов информационной

безопасности, отработка ими планов восстановлений на случай аварийных ситуаций;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- проведение расследований инцидентов во взаимодействии с соответствующими подразделениями и филиалами АО «Узнацбанк» с привлечением при необходимости правоохранительных органов;

- планирование и принятие мер по устранению инцидентов и их последствий; планирование и принятие мер по предотвращению повторного возникновения инцидентов.

12.5. Управление инцидентами информационной безопасности в АО «Узнацбанк» организуется и осуществляется ДИББ. При этом управление инцидентами безопасности информационных технологий осуществляется УИБ ДИББ, а физической безопасности – Управлением охраны ДИББ.

В региональных и районных филиалах управление инцидентами информационной безопасности осуществляется Отделом по безопасности, режиму и защите информации и Сектором автоматизации и компьютеризации во взаимодействии с ДИББ.

12.6. Фиксации и учету подлежат следующие события информационной безопасности:

- аварийные и чрезвычайные ситуации (техногенные угрозы);

- нарушение конфиденциальности, целостности и доступности информации;

- нарушение технологического процесса;

- нештатные ситуации (пожары, наводнения и иные стихийные бедствия или техногенные аварии);

- пропадание связи с внешними сетями и корпоративной связи головного офиса (основного ЦОД), резервного ЦОД, региональных и районных филиалов;

- отказ основного сетевого, серверного оборудования, средств защиты информации по любым причинам, как технического, так и программного характера;

- нарушение работы программного обеспечения информационных систем и ресурсов;

- неавторизированный или несанкционированный доступ третьих лиц к информационным системам и ресурсам;

- нарушение любых правил обработки, хранения, передачи информации;

- отказ в обслуживании DoS (Denial of Servise) и DDoS (Distributed Denial of Servise);

- выявленные средствами защиты сетевые атаки и вторжения;

- сбои (перезагрузки) в работе ЛВС, корпоративной сети, серверов и установленного на них программного обеспечения, средств защиты информации;

- аномальная сетевая активность и аномальное поведение приложений;

- подключение новых сетевых узлов и появление новых служб;

- утеря и кража ценных материальных активов, средств, носителей и самой информации;

- выявление уязвимостей;

- переустановка операционной системы или программ приложений;

- изменение аппаратной конфигурации, настроек и параметров информационной безопасности;

- выявленные неправомерные действия по сбору информации;

- выявленные опасные вирусы и вредоносные программы;

- утечка, удаление, неправомерный доступ к защищаемой информации;

- иные нарушение правил, определенных настоящей Политикой информационной безопасности.

12.7. Для выявления инцидентов информационной безопасности, связанных с применением информационных технологий, должны использоваться:

- выходные данные, предоставляемые SIEM, которая должна охватывать все средства защиты информации, используемые в АО «Узнацбанк»;

- данные системы дистанционного контроля сетевых сервисов и ресурсов, а также контроля функционирования сетевого оборудования;

- системные журналы (лог-файлы) информационных систем АО «Узнацбанк» (серверов, веб-приложений, операционных систем, СУБД, прикладных программ информационных систем и т.д.), основного сетевого оборудования (маршрутизаторов и коммутаторов ядра) и средств защиты (межсетевые экраны, системы антивирусной защиты, Центр регистрации ключей ЭЦП, средства анализа и контроля защищенности и выявления уязвимостей);

- визуальный контроль состояния работоспособности средств;

- выходные данные средств защиты информации, включая средств антивирусной защиты, межсетевых экранов, средств обнаружения и предотвращения вторжений IDPS и т.д.;

- результаты проведения внутреннего или внешнего аудита информационной безопасности;

- информация о событиях и инцидентах, о которых сообщили сотрудники и вспомогательный персонал банка;

- жалобы клиента банка по возникшим у них финансовым проблемам (кража средств, невозможность пользования банковским сервисом и др.).

12.8. Ответственными за выявление и реагирование на инциденты информационной безопасности являются:

- ЛВС, рабочие станции и сервера, сетевое оборудование головного офиса – сотрудники Отдела системного программного обеспечения Департамента информационных технологий (ДИТ) (уведомляют об инцидентах начальника ДИТ и УИБ ДИББ);

- ЛВС и рабочие станции, сервера, сетевое оборудование региональных и районных филиалов, минибанков, банкоматов – сотрудники Сектора автоматизации, компьютеризации и внедрения ИКТ (уведомляют об инцидентах Отдел по безопасности, режиму и защите информации областного

филиала);

- корпоративная сеть– сотрудники Отдела сопровождения сетевой инфраструктуры ДИТ (уведомляют об инцидентах начальника ДИТ и УИБ ДИББ);

- официальный веб-сайт АО «Узнацбанк» - ответственный сотрудник Департамента развития сети и сервиса банка (уведомляют об инцидентах УИБ ДИББ);

- информационные системы и принадлежащие им информационные ресурсы, аппаратные и программные средства – сотрудники ДИТ и Департамента розничного бизнеса (ДРБ) (уведомляют об инцидентах начальников своих департаментов и УИБ ДИББ);

- средства защиты информации (антивирус, межсетевые экраны, IDPS, Центр регистрации ключей ЭЦП и др.) – сотрудники ДИББ (уведомляют об инцидентах начальника ДИББ и УИБ ДИББ).

12.9. В УИБ ДИББ определяется сотрудник, ответственный за учет всех инцидентов информационной безопасности в АО «Узнацбанк» (далее – сотрудник, ответственное по инцидентам). В обязанности данного ответственного сотрудника входит:

1) обслуживание (администрирование) системы SIEM;

2) сбор (свод) информации об инцидентах с подразделений, региональных и районных филиалов;

3) контроль за проведением работ по устранению и ликвидации последствий инцидентов;

4) информирование начальника ДИББ о возникших инцидентах и ходе их устранений и ликвидации последствий;

5) ведение журнала учета инцидентов информационной безопасности;

6) взаимодействие с ГУП «Центр кибербезопаснсоти» при выявлении и реагировании на инциденты информационной безопасности;

7) ведение и анализ статистики по инцидентам информационной безопасности.

12.10. В журнале учета инцидентов информационной безопасности, форма которой приведена в приложении №18 к настоящей Политике, должна вноситься информация о всех инцидентах, приведших к существенным нежелательным и негативным последствиям информационной безопасности, включая аварийные (чрезвычайные) ситуации, а также инциденты, произошедших на важных критичных объектах защиты (информационные системы, в том числе система электронного документооборота, корпоративная электронная почта, официальный веб-сайт, основное коммутационное оборудование-коммутаторы ядра, маршрутизаторы, сервера IP-телефонии, видеоконференцсвязи, каналы подключения к внешним сетям и каналы корпоративной сети, банкоматы). В Журнале учета инцидентов информационной безопасности указывается дата и время события, вид события, объект защиты, с которым связано событие, и характер последствий.

12.11. О всех выявленных инцидентах информационной безопасности в региональных и районных филиалах, минибанках Отдел по безопасности,

режиму и защите информации региональных филиалов должны сообщать и предоставлять полную и объективную информацию сотруднику, ответственному по инцидентам УИБ ДИББ.

12.12. Сотрудники и персонал АО «Узнацбанк» о выявленных инцидентах информационной безопасности должны сообщать в ДИББ, Отдел по безопасности, режиму и защите информации региональных филиалов и главному специалисту по безопасности, режиму и защите информации районных филиалов. Сотрудники АО «Узнацбанк» не должны принимать несогласованные с указанными подразделениями действия по ликвидации последствий инцидентов, с тем чтобы не увеличить их последствия.

12.13. В случае возникновения событий информационной безопасности, приведших к существенным нежелательным и негативным последствиям информационной безопасности, о них должны сообщаться руководителям филиалов и руководству АО «Узнацбанк».

12.14. Руководство АО «Узнацбанк» должно немедленно уведомить Центральный банк Республики Узбекистан о происшествии в письменной или электронной форме.

12.15. В УИБ ДИББ должна быть организована работа по сбору информации от клиентов банка, по связанным у них финансовым проблемам (кража средств, невозможность пользования банковскими сервисами и др.), носящих как частный, так и общий характер. Данные жалобы клиентов банка должны рассматриваться УИБ ДИББ как инциденты информационной безопасности и реагировать на них в установленном данным разделом порядке.

12.16. По каждому инциденту информационной безопасности определяются причины возникновения инцидента, источник угрозы, оцениваются масштабы последствий, принимаются меры по устранению угрозы и ликвидации последствий инцидента. Работы по устранению последствий инцидентов организуется и координируется ДИББ с привлечением групп реагирования и использованием принятых планов восстановления. При необходимости по решению директора ДИББ к устранению последствий привлекаются дополнительные специалисты и ресурсы иных подразделений. К устранению последствий могут быть привлечены сторонние эксперты или специалисты обслуживающей организации. В случае, когда внешние эксперты или специалисты обслуживающей организации участвуют в ликвидации последствий инцидентов, с ними должно быть заключено соглашение о неразглашении конфиденциальной информации.

12.17. При реагировании на выявленные инциденты информационной безопасности сотрудник, ответственный по инцидентам УИБ ДИББ, должен взаимодействовать с ГУП «Центр кибербезопасности» в соответствии с Регламентом взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности.

12.18. Для проведения расследований инцидентов директорами ДИББ,

ДИТ и /или ДРБ, создается группа из входящих в состав этих департаментов специалистов и иных заинтересованных подразделений головного офиса, а также специалистов Отделов по безопасности, режиму и защите информации и иных заинтересованных подразделений региональных филиалов и главных специалистов по безопасности, режиму и защите информации районных филиалов при необходимости. При расследовании выявляются истинные причины инцидента, нарушители и вырабатываются рекомендации для предотвращения повторного возникновения данного инцидента. На основе данных рекомендаций указанными подразделениями принимаются и реализуются меры для предотвращения повторения инцидента.

12.19. К расследованию инцидентов с тяжкими последствиями с целью привлечения к ответственности нарушителей должны привлекаться правоохранительные органы.

12.20. Решение о проведении специального расследования инцидента, сообщение о них внешним заинтересованным сторонам и привлечение правоохранительных органов принимается руководством АО «Узнацбанк», исходя из тяжести и последствий произошедшего инцидента.

XIII. Обеспечение безопасности каналов связи

13.1. Кабели электропитания и сетевые кабели, используемые для передачи данных, необходимо защищать от вскрытия в целях исключения перехвата информации и их повреждения. Для уменьшения такого риска реализуются следующие защитные меры:

а) кабели электропитания и связи должны проводится (по возможности) под землей, в канализациях и коллекторах, а внутри зданий в коробах или защищены надлежащим образом от несанкционированного физического доступа;

б) для защиты сетевых кабелей от их несанкционированного вскрытия и перехвата данных, а также от повреждения, используются экранированные кабели, которые прокладываются так, чтобы они не проходили через общедоступные места. При отсутствии технической возможности прокладки кабелей в обход общедоступных мест, такие кабели должны укладываться в металлические короба, конструкция которых исключает возможность их несанкционированного вскрытия;

в) незадействованные разъемы сетевых кабелей, предназначенные для подключения рабочих станций, должны опечатываться или заклеиваться специальной маркой для исключения возможного несанкционированного подключения нештатных технических средств обработки информации;

г) кроссовое и коммутационное оборудования с подключенными к ней сетевыми кабелями должны размещаться в закрываемых серверных и коммутационных помещениях и в закрываемых коммутационных шкафах.

13.2. Сетевые кабели, по мере возможности, должны пролегать отдельно от электрических, чтобы исключить негативное влияние друг на друга (магнитные помехи), а также быть защищены от неавторизованных подключений или повреждений, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход

общедоступных участков.

13.3. Сетевые кабели, используемые для подключения банкоматов Uzcard и HUMO, расположенных вне зоны банка, должны быть защищены от несанкционированного доступа к ним и прокладываться в канализациях. Указанные банкоматы подключаются к ИАБС через корпоративную сеть АО «Узнацбанк». Для подключения банкоматов VISA/MasterCard к системе процессинга VISA/MasterCard ДРБ используется модемы сотовой связи с организации защищенных VPN-туннелей, организуемых VPN шлюзом доступа к системе процессинга VISA/MasterCard.

13.4. В целях обеспечения конфиденциальности информации при передаче её по внешним сетям телекоммуникаций и корпоративной сети АО «Узнацбанк» реализуются следующие защитные меры:

а) использование VPN-туннелей в корпоративной сети АО «Узнацбанк», организуемых между маршрутизаторами головного офиса (основного ЦОД) и маршрутизаторами резервного ЦОД, региональных и районных филиалов;

б) применение СКЗИ в ИАБС для криптографического шифрования информации при передаче информации по каналам связи корпоративной сети;

в) использование защищенных https-соединений с применением протоколов https, SSL/TLS при обеспечении доступа через сеть Интернет клиентов банка к веб-ресурсам Интернет-банкинга АО «Узнацбанк» (https://milliy.nbu.uz/ и https://ibank.nbu.uz/), а также сотрудников банка при доступе к ИАБС через веб-ресурс по корпоративной сети;

г) применение защищенных VPN-соединений при удаленном подключении системных и сетевых администраторов от своих рабочих станций к сетевому и серверному оборудованию, расположенном в ЦОД и филиалах, через корпоративную сеть и ЛВС АО «Узнацбанк». Для удаленного подключения применяется сетевой протокол SSH, обеспечивающий шифрованный канал и аутентификацию по ЭЦП. Организация удаленного доступа через внешнюю сеть передачи данных к внутренним информационным системам, ресурсам и оборудованию АО «Узнацбанк» не допускается.

д) использование защищенных систем передачи информации, таких как E-ijro, E-xat для обмена сообщениями (корреспонденцией) со сторонними организациями.

13.5. К системе защищенной электронной почты E-xat подключены сотрудники подразделений управления делами головного офиса, региональных и районных филиалов для обмена письменной корреспонденцией между ними.

13.6. Шифрование информации в АО «Узнацбанк» обеспечивается сертифицированными в Республике Узбекистан средствами криптографической защиты информации.

13.7. В АО «Узнацбанк» должны выполняться требования по запрещению подключения (предоставления доступа)к внешней сети (Интернет, TAS-IX, МСПД) рабочих станций, серверов, банкоматов, имеющих доступ или используемых в ИАБС. Для подключения к внешней сети сотрудники банка должны использоваться отдельные рабочие станции, которым предоставляется такой доступ.

13.8. Не допускается применение технологий Wi-Fi при построении ЛВС в АО «Узнацбанк», а также для организации точек доступа к ЛВС и корпоративной сети АО «Узнацбанк».

13.9. В региональных и районных филиалах (Центры оказания банковских услуг населению) и минибанках допускается организация сети Wi-Fi для привлечения и создания удобства клиентам. Данные Wi-Fi сети должны организовываться с выполнением следующих требований: не иметь подключение к ЛВС филиала или минибанка, корпоративной сети АО «Узнацбанк» с организацией отдельного для данной Wi-Fi сети подключения к сети Интернет (отдельная физическая сеть).

13.10. Требования по организации защищенных сетевых соединений в корпоративной сети, приведены в Положении о корпоративной сети и организации защищенных сетевых соединений согласно приложению №1 к настоящей Политике.

XIV. Распределение ответственности

14.1. Для создания и поддержания режима информационной безопасности, необходимо четкое и документальное закрепление ответственности за информационную безопасность АО «Узнацбанк» и отдельных её ресурсов, а также за выполнение определенных процедур защиты информации.

14.2. Ответственность за распределение ресурсов и внедрение процедур информационной безопасности возлагается на руководство АО «Узнацбанк» и руководителей подразделений головного офиса, руководителей региональных и районных филиалов, минибанков.

14.3. Основными обязанностями руководства правления АО «Узнацбанк» при обеспечении информационной безопасности являются:

- определение целей обеспечения информационной безопасности;
- формулировка, пересмотр и утверждение Политики информационной безопасности;
- контроль эффективности внедрения настоящей Политики;
- обеспечения четкого руководства и ощутимой административной поддержки инициативам, направленным на повышение безопасности;
- выделения необходимых средств для обеспечения информационной безопасности;
- назначение ответственных за информационную безопасность в пределах АО «Узнацбанк» и определение их обязанностей;
- инициирование планов и программ поддержания осведомленности персонала по информационной безопасности.

14.4. Непосредственная организация и эффективное функционирование СУИБ в АО «Узнацбанк» возлагается на ДИББ и Отделы по безопасности, режиму и защите информации региональных филиалов и главных специалистов по безопасности, режиму и защите информации районных филиалов (далее - подразделения информационной безопасности). Задачи и обязанности указанных подразделений в части обеспечения информационной безопасности определены в Положении о ДИББ, подразделениях и

сотрудниках, ответственных за обеспечение информационной безопасности, согласно приложению №5 к настоящей Политике.

14.5. Настоящая Политика устанавливает следующее распределение ответственности за обеспечение информационной безопасности в АО «Узнацбанк»:

- за всю деятельность по обеспечению информационной безопасности в АО «Узнацбанк» несет ответственность директор ДИББ;

- за обеспечение информационной безопасности в головном офисе АО «Узнацбанк» несет ответственность начальник УИБ ДИББ (администратор информационной безопасности АО «Узнацбанк»), в региональных и районных филиалах, а также подчиненных им мини банках–начальники Отделов по безопасности, режиму и защите информации региональных филиалов;

- за обеспечение физической безопасности в головном офисе несет ответственность начальник Управления охраны ДИББ, в региональных и районных филиалах, а также подчиненных им мининбанках – начальники Отделов по безопасности, режиму и защите информации региональных филиалов и главные специалисты по безопасности, режиму и защите информации районных филиалов;

- за обеспечение бесперебойного и нормального функционирования ЛВС АО «Узнацбанк» головного офиса АО «Узнацбанк», несут ответственность директор ДИТ и начальник Отдела системного программного обеспечения ДИТ, а также системный администратор ЛВС АО «Узнацбанк»:

- за обеспечение бесперебойного и нормального функционирования локальных серверов, ЛВС и других важных ресурсов с ограниченным доступом, физически находящихся внутри региональных и районных филиалов, а также подключаемых к ним мини банков и банкоматов несут ответственность начальники Секторов автоматизации, компьютеризации и внедрения ИКТ региональных и районных филиалов;

- за обеспечение бесперебойного и нормального функционирования корпоративной сети АО «Узнацбанк» и обмена в ней информации, её доступность и конфиденциальность, несут ответственность начальник Отдела сопровождения сетевой инфраструктуры ДИТ и сетевой администратор корпоративной сети;

- за обеспечение бесперебойного и нормального функционирования информационных систем несут ответственность директор ДИТ, начальник Управления поддержки информационных систем и системные администраторы информационных систем (за каждой информационной системой закрепляется конкретный системный администратор);

- за обеспечение бесперебойного и нормального функционирования системы процессинга VISA/MasterCard несут ответственность директор ДРБ, начальники его подразделений и системный администратор системы процессинга VISA/MasterCard;

- за нарушение конфиденциальной защищаемой информации (в любом её виде) несут персональную ответственность сотрудники банка;

- за действия, совершаемые в информационных системах

АО «Узнацбанк», несут ответственность сотрудники банка в рамках закрепленных за ними обязанностей;

- за информационную безопасность (в т.ч. физическую безопасность) рабочей станции несет ответственность сотрудник банка, которому данная рабочая станция предоставлена для исполнения служебных обязанностей;

- за пожарную и техническую безопасность, сохранность оборудования внутри каждого помещения несет ответственность сотрудник, назначенный соответствующим распоряжением руководителя структурных подразделений головного офиса, региональных и районных филиалов, мини банков АО «Узнацбанк».

14.6. Указанная в пункте 14.5 ответственность определяется в должностных обязанностях работников и других внутренних нормативных документах АО «Узнацбанк».

14.7. На время отсутствия ответственного (отпуск, болезнь, командировка и пр.) его обязанности выполняет лицо, назначенное в установленном порядке. Данное лицо приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

XV. Порядок пересмотра и актуализации политики

15.1. В настоящую Политику могут вноситься изменения и дополнения в следующих случаях:

- вступления отдельных пунктов Политики информационной безопасности в противоречие с новыми или измененными законодательными и иными нормативно-правовыми актами, нормативными документами по информационной безопасности;

- необходимости пересмотра требований обеспечения информационной безопасности;

- изменения конфигурации и состава банковской информационной инфраструктуры АО «Узнацбанк», появления новых объектов защиты информации;

- изменения состава средств защиты информации;

- изменения структуры (реорганизации) АО «Узнацбанк».

15.2. В случае вступления отдельных пунктов настоящей Политики в противоречие с новыми законодательными актами Республики Узбекистан в области защиты информации, а также иными нормативными актами АО «Узнацбанк», данные пункты утрачивают юридическую силу до момента внесения дополнений и изменений в Политику информационной безопасности АО «Узнацбанк».

15.3. Изменения и дополнения в настоящую Политику вносятся по инициативе ДИББ и утверждаются наблюдательном советом АО «Узнацбанк».

15.4. Полный пересмотр Политики информационной безопасности должен осуществляться в случае реконструкции банковской информационной инфраструктуры АО «Узнацбанк» и связанных с ней информационно-технологических процессов, реорганизации АО «Узнацбанк», влекущие изменения её структуры СУИБ.

15.5. Новая редакция Политики подлежит повторному согласованию с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и Службой государственной безопасности Республики Узбекистан.

15.6. Актуализация и оценка эффективности Политики информационной безопасности АО «Узнацбанк» осуществляется путем проведения внутреннего и внешнего аудита информационной безопасности. Аудит проводится на предмет:

- оценки выполнения требований и положений утвержденной Политики информационной безопасности;
- соответствия банковской информационной инфраструктуры АО «Узнацбанк» установленным настоящей Политикой требованиям информационной безопасности;
- оценки эффективности принятых мер, методов и средств защиты информации;
- необходимости внесения изменений, дополнений или пересмотра настоящей Политики информационной безопасности, а также внутренних нормативных документов.

15.7. Регулярность проведения внутреннего аудита должна составлять не менее 1 раза в год, а внешнего аудита – не менее 1 раза в три года.

15.8. Внутренний аудит проводится подразделениями ДИББ. Для проведения внешнего аудита информационной безопасности привлекаются сторонние организации, компетентные проводить такой аудит.

15.9. По результатам аудита и/или в процессе реализации в Политику информационной безопасности АО «Узнацбанк» могут вноситься изменения и дополнения с целью приведения её в соответствие с реальными условиями и требованиям защиты информации. Решение о внесении в Политику информационной безопасности АО «Узнацбанк» изменений и дополнений принимается директором ДИББ и выносится на согласование руководству правления АО «Узнацбанк».

15.10. Сотрудники АО «Узнацбанк» должны ознакомиться с Политикой информационной безопасности после её утверждения или пересмотра под роспись в Журнале ознакомления с Политикой информационной безопасности, форма которой приведена в приложении №19 к настоящей Политики.

Внесено:
Директор Департамента
информационной и банковской безопасности Ш. Мухамадкулов

Согласовано:
Заместитель Председателя
Правления А. Мухамедханов

Директор Департамента информационных технологий	Ш. Мусабеков
Директор Департамента юридической службы	Г. Исмаилова
Директор Департамента по работе с персоналом	Ш. Хакимов
И.о. Директор Департамента по управлению рисками	А. Соловьева
Директор Департамента розничного бизнеса	М. Раджапов
Директор Департамента развития сети и сервиса банка	Ш. Насруллаев
Директор Департамента внутреннего контроля	У. Шадиев
И.о. Директор Департамента стратегического развития банка	У. Рахимбердиев
Начальник первого отдела	Ш. Ходжаев
Начальник отдела методологии ДЮС	Т. Файзиев

ю3-695
24.11.21
пор-ка

Приложение №1
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-1 от 27.12.2021г

Положение о корпоративной сети и организации защищенных сетевых соединений

1. Общие положения

1.1 Настоящее положение определяет правила и порядок функционирования корпоративной сети АО «Узнацбанк», обеспечения на ней информационной безопасности и организации защищенных сетевых соединений.

1.2 Корпоративная сеть АО «Узнацбанк» построена с использованием арендуемых каналов сети передачи данных Главного центра информатизации Центрального банка и оператора телекоммуникаций EastTelecom.

1.3 К корпоративной сети АО «Узнацбанк» подключаются головной офис и основной ЦОД, резервный ЦОД, все областные и районные филиалы, минибанки, банкоматы и киоски АО «Узнацбанк».

К корпоративной сети АО «Узнацбанк» должны подключаться только разрешенные устройства (рабочие станции, сервера, банкоматы).

1.4 Решение о подключении к корпоративной сети структурных организаций и объектов информатизации АО «Узнацбанк» принимается руководством правления АО «Узнацбанк» и обеспечивается Отделом сопровождения сетевой инфраструктуры ДИТ. При этом должны выполняться требования защищенного подключения к корпоративной сети, которые определяются и обеспечиваются данным подразделением.

1.5 Запрещается организовывать и предоставлять доступ к внешней сети (Интернет, TAS-IX, МСПД) рабочих станций и серверов, подключенных или используемых в ИАБС.

1.6 Схема созданной АО «Узнацбанк» корпоративной сети, а также подключение её к сети передачи данных Центрального банка, сети Интернет и иным внешним сетям согласовывается с Центральным банком.

1.7 Отдел сопровождения сетевой инфраструктуры ДИТ регулярно осуществляет полный контроль и мониторинг функционирования и безопасности корпоративной сети.

2. Назначение корпоративной сети

2.1 Корпоративная сеть АО «Узнацбанк» обеспечивает:

- подключение сотрудников головного офиса, областных и районных филиалов, минибанков, а также банкоматов банка к ИАБС, сервера которых расположены в ЦОД АО «Узнацбанк»;
- подключение сотрудников головного офиса, областных и районных филиалов к БИС, сервера которых расположены в основном ЦОД АО «Узнацбанк»;

- подключение сотрудников головного офиса, областных и районных филиалов к системе электронного документооборота, сервер которой расположен в основном ЦОД АО «Узнацбанк»;

- организацию корпоративной электронной почты, IP-телефонии и видеоконференцсвязи, сервера которых расположены в основном ЦОД АО «Узнацбанк»;

- централизованный доступ к сети Интернет и TAS-IX (подключение через Uzscinet и East Telecom), организуемый через единый прокси-сервер, установленный в основном ЦОД АО «Узнацбанк»;

- подключение процессинговых серверов SWIFT и VISA/MasterCard АО «Узнацбанк» к международным системам SWIFT и VISA/MasterCard по международным каналам;

- подключение операторов денежных переводов к системам денежных переводов через сеть Интернет;

- взаимодействие ИАБС АО «Узнацбанк» с информационным системами Anor и NIBBD Центрального банка и с процессинговыми сервера SWIF и VISA/MasterCard АО «Узнацбанк»;

- подключение клиентов банка по сети Интернет к ИАБС через внешние веб-ресурсы (https://milliy.nbu.uz/ и https://ibank.nbu.uz/) для оказания услуг Интернет-банкинг;

- подключение клиентов банка по сети сотовой связи к ИАБС с применением мобильного приложения Milliy application для оказания услуг мобильный-банкинг.

3. Состав корпоративной сети

3.1 В состав корпоративной сети АО «Узнацбанк» входят:

- арендуемые каналы передачи данных операторов телекоммуникаций, а также каналы подключения корпоративной сети к внешней сети;

- сетевое телекоммуникационное оборудование (коммутаторы, маршрутизаторы, модемы), обеспечивающее подключение к корпоративной сети головного офиса, областных и районных филиалов, ЦОД и банкоматов АО «Узнацбанк»;

- межсетевые экраны, средства обнаружения и предотвращения вторжений IDPS, прокси-сервера, VPN-шлюзы АО «Узнацбанк»;

- оборудование IP-телефонии, видеоконференцсвязи и сервер корпоративной электронной почты.

4. Принцип действия корпоративной сети

4.1 Корпоративная сеть представляет собой территориально распределенную информационно-телекоммуникационную сеть.

4.2 В настоящее время корпоративная сеть АО «Узнацбанк» построена с использованием арендуемых каналов двух сетей передачи данных: Главного

организуется две разные корпоративные сети АО «Узнацбанк», между которыми идет следующее разделение трафика:

- корпоративная сеть на базе сети передачи данных Центрального банка обеспечивает подключение банкоматов HUMO к ИАБС, а также подключение сотрудников банка к системе электронного документооборота Центрального банка;

- корпоративная сеть на базе сети передачи данных EastTelecom обеспечивает подключение банкоматов Uzcard и сотрудников банка к информационным система и ресурсам АО «Узнацбанк» (ИАБС, БИС, электронный документооборота АО «Узнацбанк», корпоративная электронная почта, IP-телефония, видеоконференцсвязь), а также обеспечение их доступа к внешним сетям.

4.3 Для подключения банкоматов VISA/MasterCard к системе процессинга VISA/MasterCard ДРБ используется сеть сотовой связи и модемы сотовой связи. Система процессинга VISA/MasterCardвзаимодействует с ИАБС по ВОЛС, организуемой между основным и резервным ЦОД. Система процессинга VISA/MasterCardАО «Узнацбанк» подключается к международной системе VISA/MasterCard по отдельно организованному международному каналу передачи данных.

4.4 Корпоративная сеть АО «Узнацбанк» имеет следующие подключения к внешним сетям:

1) к сети оператора EastTelecom для:

- предоставления доступа к сети Интернет руководству правления АО «Узнацбанк» через отдельный организуемый прокси-сервер;

- предоставления доступа к сети Интернет для подключения сотрудников денежных переводов банка к системам денежных переводов через отдельный организуемый прокси-сервер;

2) к сети оператора Uzscinet через отдельный единый прокси-сервер для:

- предоставления доступа к сети Интернет и TASIX для руководства филиалов и отдельных сотрудников банка;

- внешние веб-ресурсы для оказания услуг Интернет-банкинг и для подключения клиентов мобильного банкинга.

3) к сети Главного центра информатизации Центрального банка для:

- взаимодействия ИАБС АО «Узнацбанк» с системами Anor и NIBBD Центрального банка;

- подключения отдельных сотрудников банка к системе электронного документооборота Центрального банка.

Подключение корпоративной сети АО «Узнацбанк» к внешним сетям передачи данных организуется через маршрутизатор Cisco ISR 4451 головного офиса АО «Узнацбанк». В качестве прокси-серверов используются Интернет-шлюзы Internet Control Server.

4.5 Корпоративная сеть обеспечивает централизованный доступ руководства головного офиса, областных и районных филиалов и отдельной категории сотрудников банка к TAS-IX и/или сети Интернет. Список этих сотрудников определяется руководством АО «Узнацбанк».

4.6 Не допускается на прямую подключение внутренних информационных систем (ИАБС, БИС, системы электронного документооборота, корпоративной электронной почты) к сети Интернет. Также не допускается организация удаленного доступа сотрудников банка к указанным внутренним информационным системам через внешнюю сеть.

4.7 Головной офис вместе с основным ЦОД, резервный ЦОД и областные филиалы подключаются к корпоративной сети по ВОЛС с применением маршрутизаторов Cisco ISR 4451, а районные филиалы – по ВОЛС с применением маршрутизаторов Cisco ISR 4331.

4.8 Коммутация трафика корпоративной сети обеспечивается коммутаторами ядра сети Cisco Nexus 7700, установленных в основном и резервном ЦОД. В основном и резервном ЦОД данные коммутаторы резервируются.

4.9 На базе корпоративной сети организуется единая ЛВС АО «Узнацбанк» под одним доменом с использование внутренних IP-адресов для всех подключаемых к корпоративной сети объектов (рабочие станции, сервера, банкоматы и т.д.) головного офиса, областных и районных филиалов, минибанков. Для организации единой ЛВС АО «Узнацбанк» используется домен сервер (далее - сервер ЛВС) Windows Server 2016.

4.10 Указанные в настоящем разделе сетевые средства и средства организации единой ЛВС АО «Узнацбанк» могут изменяться по мере развития и модернизации корпоративной сети АО «Узнацбанк».

5. Организация работ по сопровождению и развитию корпоративной сети

5.1 Организационное управление и эксплуатация корпоративной сетью, определение направлений и этапов её развития, а также реализация мероприятий по её развитию осуществляется Отделом сопровождения сетевой инфраструктуры ДИТ.

5.2 Управление и администрирование корпоративной сети организуется Отдел сопровождения сетевой инфраструктуры ДИТ. Для этого им назначается сетевой администратор корпоративной сети АО «Узнацбанк».

5.3 Для выполнения своих служебных обязанностей сетевой администратор корпоративной сети взаимодействует с системным администратором ЛВС АО «Узнацбанк», операторами телекоммуникаций, предоставляющими в аренду каналы передачи данных и обеспечивающие подключение к внешним сетям (TAS-IX и Интернет).

5.4 Управление работой корпоративной сети включает в себя:

- организация защищенных сетевых соединений;
- управление информационным обменом (трафиком) корпоративной сети с внешними сетями телекоммуникаций;
- управление информационными потоками (трафиком) внутри корпоративной сети;

- управление доступом сотрудников банка к информационным ресурсам и системам через корпоративную сеть, определение их полномочий и прав доступа;

- управлением доступом сотрудников банка, информационных систем и ресурсов к внешним сетям;

- подключение и отключение структурных подразделений и объектов информатизации АО «Узнацбанк» к корпоративной сети и к внешним сетям;

- техническое обслуживание и обеспечение работоспособности сетевого оборудования, сетевых ресурсов, входящих в состав корпоративной сети;

- выбор используемых в корпоративной сети программных и аппаратных средств.

5.5 Сетевой администратор корпоративной сети принимает меры по обеспечению непрерывной работоспособности корпоративной сети в соответствии с Инструкцией сетевого администратора корпоративной сети, приведенной в приложении №3 к Политике информационной безопасности АО «Узнацбанк».

5.6 Сетевой администраторы корпоративной сети обо всех случаях нарушения настоящего Положения обязан информировать начальника Отдела сопровождения сетевой инфраструктуры ДИТ. О случаях возникновения инцидентов информационной безопасности в корпоративной сети сетевой администратор корпоративной сети обязан уведомить УИБ ДИББ.

5.7 Обслуживание прокси-серверов при доступе к внешним сетям TAS-IX и Интернет, а именно управление доступом информационных систем и ресурсов, а также сотрудников банка к внешним сетям, а также обслуживание межсетевых экранов, т.е. управление доступом сотрудников банка к информационным ресурсам и системам через корпоративную сеть, определение их полномочий и прав доступа, осуществляется УИБ ДИББ.

5.8 Администрирование сервера единой ЛВС АО «Узнацбанк» осуществляется системным администратором ЛВС АО «Узнацбанк» в соответствии с Инструкцией системного администратора локальной сети АО «Узнацбанк», приведенной в приложении №4 к Политике информационной безопасности АО «Узнацбанк».

5.9 Предложения по развитию корпоративной сети формируются подразделениями ДИТ и вносятся на согласование директору ДИТ и руководству правления АО «Узнацбанк».

5.10 После согласования предложений ДИТ формируется план мероприятий по развитию корпоративной сети, который утверждается руководством правления АО «Узнацбанк». В плане мероприятий по развитию корпоративной сети должны предусматриваться мероприятия по разработке требуемой технической документации, закупка требуемого оборудования, заключение договоров, поставка и установка оборудования и т.д.

6. Развитие корпоративной сети

6.1 Основными направлениями дальнейшего развития корпоративной сети АО «Узнацбанк» являются:

- подключение АО «Узнацбанк» к МСПД с выполнением всех требований информационной безопасности при подключении к внешней сети;
- обеспечение распределения сетевой нагрузки по корпоративной сети при доступе к внутренним информационным системам сотрудников банка между корпоративными сетями, организованными на базе сетей передачи данных Главного центра информатизации Центрального банка и EastTelecom;
- обеспечение распределения сетевой нагрузки между основными и резервными ресурсами, расположенных в разных ЦОД при подключении к ним сотрудников банка, а также клиентов банка при пользования услугами Интернет-банкинг и мобильный банкинг.

7. Принципы обеспечения информационной безопасности в корпоративной сети

7.1 Обеспечение информационной безопасности корпоративной сети необходимо в целях:

- защиты информационных, сетевых и программных ресурсов от попыток несанкционированного доступа и причинения вреда;
- обеспечение конфиденциальности данных передаваемых по корпоративной сети;
- сохранности информационных ресурсов сети в случаях нарушений её работоспособности и отдельных элементов технического обеспечения;
- выполнения требований нормативных актов в области информационной безопасности.

7.2 Информационная безопасность корпоративной сети обеспечивается путём:

- использования межсетевых экранов при подключении корпоративной сети к внешним сетям в соответствии с требованиями Положения по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, привсденного в приложении №2 к Политике информационной безопасности АО «Узнацбанк»;
- применение средств IDPS при подключении корпоративной сети к внешней сети, включая МСПД, для защиты от сетевых вторжений и атак из вне;
- размещения средств обработки и хранения информации, сетевого оборудования и средств защиты информации в специальных помещениях основного и резервного ЦОД, коммутационных помещениях областных и районных филиалов, доступ к которым для посторонних лиц ограничен;
- организации защиты корпоративной сети от распространения вредоносных программ за счет мер, определенных в Инструкции по антивирусной защите, приведенной в приложении №8 к Политике информационной безопасности АО «Узнацбанк»;

- исключения несанкционированного подключения к корпоративной сети посторонних лиц и получения ими доступа к информационным ресурсам и системам через корпоративную сеть за счет осуществления мер по контролю и разграничению доступа;

- организации защищенных соединений в корпоративной сети.

7.3 Меры по обеспечению информационной безопасности корпоративной сети и эксплуатацию входящих в неё средств защиты информации осуществляются УИБ ДИББ.

8. Классификация защищенных соединений

8.1 Защищенные соединения в корпоративной сети АО «Узнацбанк» используются для обеспечения конфиденциальности и целостности передаваемой информации.

8.2 Защищенные соединения в корпоративной сети АО «Узнацбанк» классифицируются по двум критериям:

- уровню их организации;
- применяемым технологиям защиты.

8.3 По уровню организации защищенные соединения в корпоративной сети АО «Узнацбанк» классифицируются:

1) Защищенные соединения для организации связи и обмена информацией между головным офисов (основной ЦОД), резервным ЦОД, областными и районными филиалами.

2) Защищенные соединения для подключения банкоматов VISA/MasterCard через сеть сотовой связи к системе процессинга VISA/MasterCard АО «Узнацбанк».

3) Защищенные соединения при подключении сотрудников АО «Узнацбанк» к информационным системам АО «Узнацбанк» (ИАБС, БИС, система электронного документооборота) через корпоративную сеть АО «Узнацбанк».

4) Защищенные соединения для обеспечения доступа через сеть Интернет клиентов банка к веб-ресурсам Интернет-банкинга АО «Узнацбанк».

5) Защищенные соединения для удаленного подключения системных и сетевых администраторов от своих рабочих станций к сетевому и серверному оборудованию, расположенном в ЦОД и филиалах, через корпоративную сеть и ЛВС АО «Узнацбанк».

8.4 По применяемым технологиям защиты защищенные соединения в корпоративной сети АО «Узнацбанк» классифицируются:

1) защищенные соединения с применением технологий VPN;
2) защищенные соединения с применением протоколов https, SSL/TLS;
3) защищенные соединения с применением СКЗИ;
4) защищенные соединения с применением сетевого протокола SSH.

9. Принципы организации и использование защищенных соединений в корпоративной сети

9.1 В корпоративной сети АО «Узнацбанк» организуются следующие защищенные соединения:

а) Защищенные соединения в корпоративной сети с организацией VPN-туннелей между маршрутизаторами головного офиса (основного ЦОД) и маршрутизаторами резервного ЦОД, областных и районных филиалов.

Данные защищенные соединения организуются с применением VPN-технологий и с использованием протокола IPSec.

Данные защищенные соединения организуются и используются для защищенного обмена информацией в корпоративной сети между головным офисов (основной ЦОД), резервным ЦОД, областными и районными филиалами.

Используются сотрудниками АО «Узнацбанк».

Указанные защищенные соединения в корпоративной сети обеспечиваются Отделом сопровождения сетевой инфраструктуры ДИТ.

б) Защищенные VPN-соединения при подключении банкоматов VISA/MasterCard через сеть сотовой связи к системе процессинга VISA/MasterCard АО «Узнацбанк».

Организуются с применением VPN-технологий и с использованием протокола IPSec и предназначены для защищенного обмена информацией между банкоматами и процессинговым сервером VISA/MasterCard АО «Узнацбанк».

Указанные защищенные соединения обеспечиваются ДРБ.

в) Использование защищенных https-соединений с применением протоколов https, SSL/TLS при подключении сотрудников к информационным системам: ИАБС, БИС и системе электронного документооборота через веб-приложения данных систем.

Организуются для защищенного обмена информацией между рабочими станциями и информационными системами через корпоративную сеть АО «Узнацбанк».

Используются сотрудниками АО «Узнацбанк».

Ответственными за их организацию являются системные администраторы информационных систем АО «Узнацбанк».

г) Использование защищенных https-соединений с применением протоколов https, SSL/TLS при обеспечении доступа внешних пользвателей (клиенты банка) через сеть Интернет к веб-ресурсам АО «Узнацбанк» - веб-ресурсам Интернет-банкинга АО «Узнацбанк» (https://milliy.nbu.uz/ и https://ibank.nbu.uz/).

Используются внешними пользователями – клиенты банка.

Предназначены для защищенного обмена информацией между рабочими станциями клиентов банка с веб-приложениями Интернет-банкинга.

Ответственным за их организацию является системный администратор ИАБС.

д) Защищенные соединения с применением СКЗИ при обмене информацией между рабочими станции сотрудников банка и сервером ИАБС

через корпоративную сеть.

Указанные защищенные соединения в корпоративной сети обеспечиваются УИБ ДИББ.

е) Применение защищенных VPN-соединений при удаленном подключении системных и сетевых администраторов со своих рабочих станций к сетевому и серверному оборудованию, расположенном в ЦОД и филиалах, через корпоративную сеть и ЛВС АО «Узнацбанк». Для удаленного подключения применяется сетевой протокол SSH, обеспечивающий шифрованный канал и аутентификацию по ЭЦП.

Ответственность за их организацию лежит на системных и сетевых администраторов.

9.2 Контроль за организацией указанных в пункте 9.1 защищенных соединений в корпоративной сети АО «Узнацбанк» возлагается на УИБ ДИББ.

Приложение №2
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-в от 27.12.2021г

Положение по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование

1. Общие положения

1.1 Настоящее Положение разработано в целях регулирования механизма и правил обеспечения информационной безопасности на уровне сетевой инфраструктуры, а также путем управления доступа к корпоративной сети и внешним сетям АО «Узнацбанк», информационным ресурсам и системам с использованием межсетевых экранов, прокси-серверов.

1.2 Положение по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование излагает основные принципы организации защиты корпоративной сети, единой ЛВС АО «Узнацбанк», информационных систем и ресурсов от несанкционированного доступа на сетевом уровне.

2. Термины, определения и сокращения

2.1 В настоящем Положении применены следующие термины и их определения:

внешняя сеть - неподконтрольные АО «Узнацбанк» сети, включая сеть Интернет (TAS-IX), МСПД и др.;

зона DMZ - специальная зона, где размещены подконтрольные АО «Узнацбанк» сервера и системы хранения данных информационных систем;

канальный (второй) уровень модели OSI - физическая адресация на уровне коммутации;

межсетевой экран - локальное (однокомпонентное) или функционально–распределенное программное (программно–аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в систему и/или выходящей из системы;

модель OSI - базовая эталонная модель сетевого взаимодействия открытых информационных систем, которая состоит из 7 уровней, из них первые три относятся к сетевой инфраструктуре;

сетевая инфраструктура - часть корпоративной сети АО «Узнацбанк», включающая в себя линии связи, а также коммутационные устройства, обеспечивающие логическую связь между рабочими станциями и серверами;

сетевой (третий) уровень модели OSI - определение маршрута и логическая адресация на уровне IP-протокола;

физический (первый) уровень модели OSI - работа со средой передачи данных, сигналами и двоичными данными.

2.2 В настоящем Положении используются следующие сокращения:

DMZ (Demilitarized Zone)– демилитаризованная зона;

IDPS (Intrusion Detection & Prevention System) – средства (система) обнаружения и предотвращения вторжений;

VISA/MasterCard– международные платежные системы,

ПО – программное обеспечение;

ЦОД – центр обработки данных;

3. Общие требования безопасности на уровне сетевой инфраструктуры

3.1 Защита сетевой инфраструктуры основывается на защите каждого уровня модели OSI - физического, канального и сетевого и выше.

3.2 Физическая защита состоит в обеспечении безопасности среды передачи данных - витых и оптических кабелей, используемых в АО «Узнацбанк».

3.3 Защита на канальном уровне строится на основе коммутаторов с соответствующими функциями для обеспечения безопасности, которым относятся:

- предоставление списка доступа ACL (IP, MAC, VLAN);
- ограничение доступа на уровне порта (Port Security);
- функции борьбы с подменами адресов (DHCP snooping, Dynamic ARP inspection, IP source guard);
- механизм борьбы с широковещательными штормами (Storm Control);
- защита уровня управления (Control Plane Policing).

3.4 Защита на сетевом уровне строится с помощью модулей экранирования, для разграничения доступа к защищенной ЛВСАО «Узнацбанк», его сегментам и ресурсам.

3.5 В АО «Узнацбанк» применяются аппаратно-программные межсетевые экраны нового поколения осуществляющие фильтрацию данных (пакетов и соединений) на различных уровнях семиуровневой модели OSI (от сетевого уровня до уровня приложений) в соответствии с заданными правилами сетевой безопасности, идентификацию и контроль приложений по любому порту, скрытие адреса (трансляция IP-адресов) и структуры защищаемой сети для внешних пользователей (сегментирование и маскирование сети).

3.6 На границе подключения корпоративной сети к внешней сети применяются прокси-сервера (Интернет-шлюзы), обеспечивающие управление доступом к внешней сети, включая авторизацию при доступе, фильтрацию по URL-адресам, сетевым сервисам и контенту, а также пропуск требуемого для сотрудника банка и информационных систем и ресурсов АО «Узнацбанк» трафика, а именно защиту (экранирование) на сеансовом и прикладном уровне OSI.

3.7 Защита от сетевых вторжений и атак начиная со 2-го и выше уровней OSI обеспечивается применением сетевых средств обнаружения и предотвращения вторжений (IDPS).

Сетевые средства IDPS должны обнаруживать сетевые вторжения и атаки с использованием сигнатурного и поведенческого метода анализа, а также предотвращать их действие.

При эксплуатации средств IDPS должно быть обеспечено периодическое обновление используемых в них баз сигнатур атак.

Сетевые средства IDPS должны применяться для защиты от сетевых вторжений и атак на границе подключения:

- корпоративной сети АО «Узнацбанк» к сети Интернет (TAS-IX) и МСПД;
- подключение DMZ основного и резервного ЦОД к корпоративной сети;
- подключение резервного ЦОД (системы процессинга VISA/MasterCard АО «Узнацбанк») к внешней сети.

В качестве средств IDPS используются аппаратно-программные межсетевые экраны нового поколения, реализующие функции обнаружения и предотвращения вторжений, мониторинга и контроля приложений (AVC), защиту от вредоносного ПО (Antivirus) и URL-фильтрацию.

4. Общие требования по обеспечению информационной безопасности с применением межсетевых экранов

4.1 Внедряемые в АО «Узнацбанк» межсетевые экраны должны:

- обеспечивать безопасность защищаемой сети или её сегмента и полный контроль над внешними подключениями и сеансами связи;
- обладать мощными и гибкими средствами управления для полной и простой реализации Политики информационной безопасности АО «Узнацбанк»;
- обеспечивать простую реконфигурацию системы при изменении структуры сети;
- работать незаметно для пользователей сети и не затруднять выполнение ими легальных действий;
- работать достаточно эффективно и своевременно обрабатывать весь входящий и исходящий трафик в «пиковых» режимах (обладать требуемой пропускной способностью с учетом развития);
- обладать свойствами самозащиты от любых несанкционированных воздействий;
- осуществлять протоколирование событий и регистрацию всех действий, имеющих отношение к безопасности.

4.2 Межсетевые экраны устанавливаются на границе подключения:

- корпоративной сети к сети Интернет (TAS-IX) и МСПД;
- DMZ основного ЦОД к ЛВС головного офиса и корпоративной сети;
- DMZ резервного ЦОД к корпоративной сети;
- резервного ЦОД (системы процессинга VISA/MasterCard АО «Узнацбанк») к внешней сети.

4.3 Межсетевые экраны, указанные в пункте 4.1 должны быть не ниже 3 класса защищенности в соответствии с государственным стандартом O‘zSt

2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации».

4.4 Корпоративная сеть должна быть защищена от сети Интернет (TAS-IX) и МСПД (внешние сети) с применением аппаратно-программного межсетевого экрана, который должен обеспечивать выполнение следующих требований при его настройке:

- блокировать доступ в корпоративную сеть с внешней сети за исключением клиентов Интернет-банкинг и мобильного банкинга для оказания интерактивных банковских услуг и почтового трафика сотрудников внешней электронной почты;
- предоставлять доступ к внешней сети только рабочим станциям сотрудников и информационным системам АО «Узнацбанк», имеющих разрешение на такой доступ, а также управлять этим доступом;
- фильтровать запросы и трафик по портам, протоколам, IP-адресам, URL-адресам в соответствии с правилами фильтрации для выполнения требований Политики информационной безопасности АО «Узнацбанк»;
- обеспечивать трансляцию сетевых адресов (NAT).

4.5 Для разграничения DMZ основного и резервного ЦОД от ЛВС и корпоративной сети АО «Узнацбанк» должны применяться аппаратно-программные межсетевые экрана, обеспечивающие фильтрацию трафика и запросов, а также управление доступом к определенным информационным системам и ресурсам, размещенным в DMZ. Настройки этих межсетевых экранов в основном и резервном ЦОД должны быть идентичными.

4.6 Для разграничения системы процессинга VISA/MasterCard АО «Узнацбанк» (резервный ЦОД) с внешней сетью должны применяться аппаратно-программные межсетевые экрана, обеспечивающие фильтрацию трафика и запросов, а также управление доступом к системе по IP-адресам и MAC-адресам банкоматов.

4.7 Перед внедрением межсетевые экраны должны пройти испытания на контрольных стендах и опытную эксплуатацию в соответствии с разделом 6 настоящего Положения.

4.8 Эксплуатацию (техническое обслуживание, изменение настроек) межсетевых экранов осуществляют специалисты УИБ ДИББ.

5. Процедуры внесения изменений в настройку и конфигурацию межсетевых экранов

5.1 Изменения в настройку и конфигурацию межсетевых экранов вносятся обслуживающими их специалистами в случаях:

- необходимости изменения правил фильтрации или установления ограничений по отдельным соединениям и доступу по требованию руководства или в связи с изменениями Политики информационной безопасности;
- изменения конфигурации ЛВС, добавления новых приложений, устройств или пользователей;

- на основании заявки руководителя подразделения на имя директора ДИББ о необходимости внесения изменений в межсетевой экран;

- возникновения сбоев или выявления атак злоумышленников и др.

5.2 О каждом внесенном изменении в настройку и конфигурацию межсетевых экранов администраторы обязаны уведомить начальника УИБ ДИББ.

5.3 Вносимые изменения в настройку и конфигурацию межсетевых экранов должны фиксироваться администраторами в журналах, форма которой приведена в приложении к настоящему Положению.

Лица и подразделения, на основании заявок которых внесены изменения в межсетевой экран, должны быть поставлены в известность УИБ ДИББ письменно или по электронной почте.

5.4 Отдельным назначенным сотрудником УИБ ДИББ, не являющимся администратором, обслуживающим межсетевой экран, должна ежемесячно проводиться проверка внесений изменений в настройку и конфигурацию межсетевых экранов путем просмотра журнала регистрации внесения изменений в межсетевой экран с журналом действий администратора, который ведется межсетевым экраном.

5.5 Также УИБ ДИББ проводит аудит и контроль настроек межсетевых экранов не реже одного раза в полгода. В ходе аудита проверяются соблюдение требований эксплуатации межсетевых экранов, правильность настроек, а также просмотр регистрационных и системных журналов.

В случае, если УИБ ДИББ не имеет непосредственного доступа на межсетевой экран, подразделением банка, эксплуатирующим его, должна быть предоставлена такая информация по первому требованию УИБ ДИББ.

6. Порядок проведения испытаний и опытной эксплуатации на контрольных стендах

6.1 Целью проведения испытаний и опытной эксплуатации межсетевых экранов является подтверждение соответствия межсетевых экранов требованиям нормативных документов, а также проверку реализации требуемых правил фильтрации.

6.2 Для проведения испытаниий и опытной эксплуатации межсетевых экранов создается контрольный стенд, который должен предоставлять администратору возможность генерации пакета (установления соединения) с произвольньми параметрами и проводить анализ влияния настроек межсетевого экрана на результат испытаний (пропушен ли пакет через межсетевой экран, установлено ли соединение).

Простейшая схема контрольного стенда включает в себя генератор пакетов (соединений), межсетевой экран, анализатор трафика. Для проверки установления соединений генератор пакетов должен иметь возможность установки соединений, а анализатор трафика - универсальный сервер, способный обслуживать любой произвольно заданный порт или прикладной сервис.

6.3 В процессе испытаний и опытной эксплуатации администратору

необходимо осуществлять генерацию и анализ результата прохождения пакета или установления соединения «по разные стороны» межсетевого экрана (то есть генератор пакетов и анализатор трафика должны располагаться в разных сторонах).

На основе анализа полученных результатов прохождения тестового трафика через межсетевой экран и их сопоставления с результатами, при которых средство считается соответствующим определенному требованию, формируется вывод о корректности реализации в межсетевом экране проверяемого механизма защиты.

6.4 Испытания межсетевого экрана провидится до тех пор, пока не будут проверены все требуемые контрольные функции и правила фильтрации. Срок прохождения опытной эксплуатации межсетевого экрана должен быть не менее одного месяца.

6.5 После успешного прохождения испытания и опытной эксплуатации межсетевой экран допускается к эксплуатации.

7. Порядок ввода изменений в эксплуатацию

7.1 Перед подключением межсетевых экранов должна быть произведена их настройка в соответствии с требованиями настоящего Положения и Политики информационной безопасности АО «Узнацбанк».

7.2 При эксплуатации межсетевых экранов должны обеспечиваться:

- систематический контроль и диагностика функционирования межсетевых экранов, а также отслеживание выполнения контрольных функций межсетевыми экранами;
- изменение настроек и конфигурации межсетевых экранов в случаях, указанных в разделе 5 настоящего Положения;
- ежедневная проверка настроек и конфигурации межсетевых экранов на соответствие установленным требованиям фильтрации и выполнения контрольных функций;
- сохранение последних настроек межсетевых экранов (создание электронного архива настроек);
- восстановление функционирования при выходе из строя межсетевого экрана или замена его с восстановлением всех последних настроек и конфигурации.

7.3 В порядок эксплуатации межсетевых экранов могу быть внесены изменения с целью повышения контроля за функционированием межсетевых экранов в ситуациях повышения объема пропускаемого трафик или, увеличения частоты выхода из строя межсетевого экрана и др.

7.4 Изменения в эксплуатацию межсетевых экранов вводятся УИБ ДИББ по согласованию с директором ДИББ и должны выполняться специалистами, обслуживающими межсетевые экраны.

7.5 Специалисты, обслуживающие межсетевые экраны, должны ежедневно просматривать журналы безопасности и статистику событий межсетевого экрана, а также анализировать электронные протоколы межсетевых экранов для обнаружения внешних атак.

7.6 В случае выявления внешних атак специалисты, обслуживающие межсетевые экраны, обязаны уведомить об этом УИБ ДИББ. О всех выявленных внешних атаках УИБ ДИББ обязан сообщать в Центральный банк в тот же день, когда обнаружены внешние атаки.

8. Ответственность

8.1 Администраторы, обслуживающие и выполняющие эксплуатацию межсетевых экранов, несут ответственность за соблюдение установленных настоящим Положением требований.

8.2 УИБ ДИББ осуществляет контроль за выполнением требований настоящего Положения.

Приложение
к Положению по обеспечению
информационной безопасности на
уровне сетевой инфраструктуры и
межсетевое экранирование

Форма журнала
регистрации внесения изменений в настройку и конфигурацию межсетевого экрана

№	Дата и время	Внесенные изменения	Причина внесений изменений

Приложение №3
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-в от 27.12.2021г.

Инструкция сетевого администратора корпоративной сети

1. Общие положения

1.1 Настоящая Инструкция разработана в целях определения порядка и правил администрирования корпоративной сети АО «Узнацбанк», обязанностей сетевого администратора корпоративной сети по поддержанию беспрерывной её работы и должного уровня её информационной безопасности.

1.2 Обязанности по администрированию корпоративной сети возлагаются на сетевого администратора корпоративной сети (далее – сетевой администратор), а в его отсутствие на заместителя сетевого администратора, которые являются сотрудниками Отдела сопровождения сетевой инфраструктуры ДИТ и назначаются директором ДИТ.

1.3 Права и обязанности сетевого администратора определяются настоящей Инструкцией и прописываются в его должностной инструкции.

В период отсутствия на работе сетевого администратора по болезни или во время его трудового отпуска и командировки, права, обязанности и ответственность сетевого администратора, определенных настоящей Инструкцией, возлагаются на его заместителя.

1.4 Сетевой администратор и его заместитель должны иметь опыт работы в сфере ИКТ не менее 3-х лет.

1.5 Требования сетевого администратора, а в период его отсутствия требования заместителя сетевого администратора, связанные с выполнением ими своих функций, обязательны для исполнения всеми пользователями корпоративной сети, а также сотрудниками, обеспечивающими эксплуатацию сетевого оборудования, входящие в состав корпоративной сети (сотрудники Отдела сопровождения сетевой инфраструктуры ДИТ, Сектора автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов).

1.6 Сетевой администратор в своей деятельности руководствуется:

- Политикой информационной безопасности;
- приказами и распоряжениями АО «Узнацбанк»;
- актами законодательства, правилами внутреннего трудового распорядка;
- методиками и руководствами по обслуживанию, администрированию и обеспечению информационной безопасности корпоративной сети;
- настоящей Инструкцией.

2. Обязанности сетевого администратора

2.1 Сетевой администратор должен знать:

- в совершенстве применяемые информационные технологии в корпоративной сети;
- руководства по эксплуатации сетевого оборудования корпоративной сети;
- топологию и схему организации корпоративной сети;
- требования по обеспечению информационной безопасности в корпоративной сети;
- методы выявления каналов утечки информации в корпоративной сети;
- методы планирования, организации и проведения работ по организации защищенных соединений в корпоративной сети;
- методы и технологии управления сетевыми устройства и сетевыми потоками;
- правила и нормы охраны труда, техники безопасности, производственной санитарии и противопожарной защиты.

2.2 Для обеспечения нормального функционирования и информационной безопасности корпоративной сети сетевой администратор организовывает и координирует работу сотрудников Отдела сопровождения сетевой инфраструктуры ДИТ, Сектора автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов, ответственных за обслуживание сетевого оборудования, входящего в состав корпоративной сети.

2.3 Сетевой администратор обязан:

- контролировать действия сотрудников Отдела сопровождения сетевой инфраструктуры ДИТ, Сектора автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов при обслуживании ими сетевого оборудования, входящих в состав корпоративной сети;
- организовывать и обеспечивать подключение новых структурных подразделений и объектов информатизации к корпоративной сети;
- обеспечивать распределение (управление) сетевого трафика по каналам корпоративной сети, внешним каналам и между информационными системами и ресурсами, а также управление таблицей маршрутизации;
- обеспечивать защищенное подключение корпоративной сети к внешним сетям;
- контролировать работоспособность технических, программных, сетевых ресурсов, входящих в состав корпоративной сети;
- организовывать и проводить работы по установке, настройке и конфигурированию требуемого аппаратного и программного обеспечения корпоративной сети;
- осуществлять контроль за эксплуатацией (установку, настройку, управление и техническое обслуживание) технических, программных, сетевых ресурсов, входящих в состав корпоративной сети;

- разрабатывать и реализовывать планы и графики проведения профилактических работ по обслуживанию корпоративной сети;

- организовывать и проводить работы по поддержке кабельной инфраструктуры, в т.ч. подключение сетевых средств и средств обработки информации к корпоративной сети, поиск и исправление повреждений в кабельной системе;

- выявлять и проводить работы по своевременному устранению различных отклонений в работе корпоративной сети;

- оперативно и эффективно реагировать на события, связанные с нарушением информационной безопасности в корпоративной сети;

- анализировать данные журналов учета работы корпоративной сети с целью выявления возможных нарушений требований защиты;

- контролировать физическую сохранность средств и оборудования корпоративной сети;

- не допускать подключение к корпоративной сети, а также к работе на серверах и сетевом оборудовании корпоративной сети посторонних лиц;

- взаимодействовать с оператором телекоммуникаций по обеспечению им бесперебойности работы предоставленных в аренду каналов передачи данных и каналов, обеспечивающих подключение корпоративной сети к внешней сети;

- осуществлять периодически не менее одного раза в месяц контрольные проверки сетевого оборудования корпоративной сети, тестирование правильности их функционирования. Указанные проверки и тесты проводятся согласно плану-графику проведения профилактических работ, который ежегодно утверждается начальником Отдела сопровождения сетевой инфраструктуры ДИТ;

- подготавливать и вносить предложения по развитию инфраструктуры корпоративной сети и повышения уровня её защищенности;

- осуществлять регулярное резервное копирование конечных настроек сетевого оборудования корпоративной сети, а также резервирование основного сетевого оборудования;

- ежемесячно предоставлять начальнику Отдела сопровождения сетевой инфраструктуры ДИТ отчет о состоянии функционирования и обеспечения информационной безопасности корпоративной сети, а также незамедлительно сообщать о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации;

- уведомлять УИБ ДИББ о фактах возникновения различных инцидентов информационной безопасности в корпоративной сети и проводить согласованные действия по устранению их последствий и восстановлению функционирования;

- обеспечивать контроль за выполнением сотрудниками АО «Узнацбанк» требований настоящей Политики при пользовании корпоративной сетью.

2.4 Сетевому администратору и сотрудникам, осуществляющим эксплуатацию сетевого оборудования корпоративной сети, запрещается:

- оставлять свои рабочие станции без контроля, в том числе в рабочем состоянии;

- разглашать информацию о конфигурации и настройка сетевого оборудования;

- фиксировать пароли пользователей корпоративной сети на любых носителях информации, а также сообщать их кому бы то ни было, кроме самих сотрудников.

3. Права сетевого администратора

3.1 Сетевой администратор имеет право:

- участвовать в любых проверках корпоративной сети;

- знакомиться с проектами решений руководства, касающихся его деятельности, обеспечения работы и развития корпоративной сети АО «Узнацбанк»;

- взаимодействовать с УИБ ДИББ по вопросам обеспечения информационной безопасности в корпоративной сети и управлением доступа пользователей к информационным системам, ресурсам и внешним сетям;

- взаимодействовать с системным администратором ЛВС АО «Узнацбанк» по вопросам подключения и управления доступом сотрудников банка к корпоративной сети;

- вносить предложения по совершенствованию работы и обеспечению информационной безопасности корпоративной сети;

- устанавливать и изменять по согласованию с директором ДИТ правила пользования корпоративной сетью АО «Узнацбанк»;

- повышать уровень квалификации и проходить обучение за счет средств АО «Узнацбанк».

4. Ответственность сетевого администратора

4.1 Сетевой администратор несет ответственность за:

- неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных настоящей Инструкцией;

- качество проводимых им работ по обеспечению функционирования корпоративной сети АО «Узнацбанк»;

- нарушение правил техники безопасности.

Приложение №4
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-1 от 27.12.2021г

Инструкция системного администратора локальной сети АО «Узнацбанк»

1. Общие положения

1.1 Настоящая Инструкция разработана в целях определения порядка и правил администрирования единой ЛВС АО «Узнацбанк», обязанностей системного администраторов ЛВС по поддержанию беспрерывной её работы и должного уровня их информационной безопасности.

1.2 Обязанности по администрированию ЛВС «Узнацбанк» возлагается на системного администратора ЛВС (далее – администратор ЛВС), который является сотрудником Отдела системного программного обеспечения ДИТ и назначается директором ДИТ.

1.3 Права и обязанности администратора ЛВС определяются настоящей Инструкцией и прописываются в его должностной инструкции.

В период отсутствия на работе администратора ЛВС по болезни или во время трудового отпуска и командировки, их права, обязанности и ответственность, определенных настоящей Инструкцией, возлагаются на его заместителя.

1.4 Администратор ЛВС и его заместитель должны иметь высшее образование и опыт работы в сфере ИКТ не менее 3-х лет.

1.5 Требования администратора ЛВС, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками АО «Узнацбанк», являющихся пользователями ЛВС.

1.6 Администратор ЛВС в своей деятельности руководствуется:

- Политикой информационной безопасности;
- приказами и распоряжениями АО «Узнацбанк»;
- актами законодательства, правилами внутреннего трудового распорядка;
- методиками и руководствами по обслуживанию, администрированию и обеспечению информационной безопасности ЛВС;
- настоящей Инструкцией.

2. Обязанности администратора ЛВС

2.1 Администратор ЛВС должен знать:

- в совершенстве применяемые информационные технологии в ЛВС АО «Узнацбанк»;
- руководства по эксплуатации сервера ЛВС АО «Узнацбанк»;
- требования по обеспечению информационной безопасности ЛВС АО «Узнацбанк», серверов и рабочих станций, подключаемых к ЛВС АО «Узнацбанк»;

- топологию, схему организации ЛВС АО «Узнацбанк» и маршруты прокладки сетевых кабелей ЛВС;

- методы выявления каналов утечки информации в ЛВС АО «Узнацбанк»;

- методы и технологии управления сетевыми устройства и сетевыми потоками в ЛВС АО «Узнацбанк»;

- правила и нормы охраны труда, техники безопасности, производственной санитарии и противопожарной защиты.

2.2 Администратор ЛВС обязан:

- обеспечивать работоспособность и надежное функционирование сервера ЛВСАО «Узнацбанк»;

- осуществлять настройку, эксплуатацию (установка и настройка программного обеспечения, техническое обслуживание аппаратного обеспечения) сервера ЛВС АО «Узнацбанк»;

- заводить учетные записи подключаемых к ЛВС АО «Узнацбанк» сотрудников и сетевых устройств, предоставлять сотрудникам банка реквизиты доступа к ЛВС АО «Узнацбанк» и предоставлять им соответствующие полномочия и права доступа к сетевым информационным ресурсам и системам;

- управлять доступом к ЛВС АО «Узнацбанк» сотрудников и подключенных к ней сетевых устройств;

- обеспечивать выполнения требований по недопущению несанкционированного подключения и доступа к ЛВС АО «Узнацбанк»;

- контролировать физическую сохранность сервера ЛВС АО «Узнацбанк», а также обеспечивать сохранность, защиту и своевременное обновление программного обеспечения сервера ЛВС АО «Узнацбанк»;

- анализировать данные журналов учета работы ЛВС АО «Узнацбанк» с целью выявления возможных нарушений требований защиты;

- обеспечивать резервирование сервера ЛВС АО «Узнацбанк» и резервное копирование информации, важной для работы и функционирования сервера ЛВС АО «Узнацбанк»;

- разрабатывать и выполнять планы и графики проведения профилактических работ по обслуживанию ЛВС АО «Узнацбанк»;

- осуществлять периодически не менее одного раза в месяц контрольные проверки сервера ЛВС АО «Узнацбанк», тестирование правильности его функционирования. Указанные проверки и тесты проводятся согласно плану-графику проведения профилактических работ, который ежегодно утверждается начальником Отдела системного программного обеспечения ДИТ;

- выявлять и проводить работы по своевременному устранению различных отклонений в работе ЛВС;

- устанавливать на рабочих станциях и серверах все требуемое программное обеспечение, включая операционную систему;

- осуществлять ремонт и восстановление работоспособности или замену вышедших из строя рабочих станций и серверов;

- выполнять работы по поддержке кабельной инфраструктуры, в т.ч.

подключать сетевые средства и средства обработки информации к ЛВС, искать и исправлять повреждения в кабельной системе;

- обеспечивать контроль и восстановление связи ЛВС с корпоративной и внешней сетью АО «Узнацбанк» во взаимодействие с сетевым администратором корпоративной сети;

- выполнять требования сетевого администратора корпоративной сети при подключении ЛВС к корпоративной и внешней сети

- подготавливать и вносить предложения по развитию инфраструктуры ЛВС АО «Узнацбанк» и повышения уровня их защищенности;

- ежемесячно предоставлять начальнику Отдела системного программного обеспечения ДИТ отчет о состоянии функционирования и обеспечения информационной безопасности ЛВС АО «Узнацбанк», а также незамедлительно сообщать о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации;

- оперативно и эффективно реагировать на события, связанные с нарушением информационной безопасности в ЛВС и сообщать о них директору ДИТ и УИБ ДИББ;

- обеспечивать контроль за выполнением сотрудниками АО «Узнацбанк» требований настоящей Политики при пользовании ЛВС АО «Узнацбанк» и корпоративной сетью.

2.3Для выполнения своих обязанностей администратор ЛВС должен взаимодействовать с:

1) сетевым администраторов корпоративной сети в части обеспечения подключения ЛВС АО «Узнацбанк» к корпоративной сети и внешним сетям, а также при подключении новых объектов информатизации к ЛВС АО «Узнацбанк»;

2) сотрудниками Отдела сопровождения сетевой инфраструктуры ДИТв части:

- обеспечение функционирования и настроек сетевого оборудования ЛВС в головном офисе;

- подключения рабочих станций и сетевого оборудования к ЛВС в головном офисе;

- выполнения работ по поддержке кабельной инфраструктуры, поиску и устранению повреждений в кабельной системе головного офиса;

3) сотрудниками Отдела системного программного обеспечения ДИТ в части обеспечения настроек и установки программного обеспечения на рабочих станциях и серверах, подключаемых к ЛВС в головном офисе;

4) сотрудниками Сектора автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов в части:

- обеспечение функционирования и настроек сетевого оборудования ЛВС АО «Узнацбанк» в областных и районных филиалах;

- подключения рабочих станций, сетевого оборудования и банкоматов к ЛВС АО «Узнацбанк» в областных и районных филиалах;

- выполнения работ по поддержке кабельной инфраструктуры, поиску и устранению повреждений в кабельной системе областных и районных филиалов;

5) сотрудниками УИБ ДИББ по вопросам обеспечения информационной безопасности в ЛВС АО «Узнацбанк».

2.4 Администратору ЛВС запрещается:

- оставлять свою рабочую станцию без контроля, в том числе в рабочем состоянии;
- фиксировать учетные данные на любых носителях информации, а также сообщать их кому бы то ни было, кроме самих сотрудников;
- устанавливать на сервере ЛВС АО «Узнацбанк» нештатное программное обеспечение и обеспечивать его нецелевое использование.

3. Права администратора ЛВС

3.1 Администратор ЛВС имеет право:

- отключать от ЛВС АО «Узнацбанк» и/или корпоративной сети сотрудников, осуществивших несанкционированный доступ к защищаемым ресурсам ЛВС АО «Узнацбанк» или корпоративной сети или нарушивших другие требования по безопасности информации;
- участвовать в любых проверках ЛВСАО «Узнацбанк»;
- знакомиться с проектами решений руководства, касающихся его деятельности, обеспечения работы и развития ЛВС АО «Узнацбанк»;
- вносить предложения по совершенствованию работы и обеспечению информационной безопасности ЛВС АО «Узнацбанк»;
- устанавливать и изменять по согласованию с начальником Отдела системного программного обеспечения ДИТ правила пользования ЛВС АО «Узнацбанк»;
- повышать уровень квалификации и проходить обучение за счет средств АО «Узнацбанк».

4. Ответственность администратора ЛВС

4.1 Администратор ЛВС несет ответственность за:

- неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных настоящей Инструкцией;
- качество проводимых ими работ по контролю действий пользователей при работе в ЛВС, а также по поддержанию нормального и устойчивого функционирования и установленного уровня защиты ЛВС АО «Узнацбанк»;
- нарушение правил техники безопасности.

Приложение №5
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 от 27.12.2021г

Положение о ДИББ, подразделениях и сотрудниках, ответственных за обеспечение информационной безопасности

1. Общие положения

1.1 Настоящая Инструкция разработана в целях установления и распределения обязанностей между подразделениями и сотрудниками, ответственными за обеспечение информационной безопасности в АО «Узнацбанк».

1.2 Организация и координация работ по обеспечению информационной безопасности в АО «Узнацбанк» возлагаются на ДИББ.

По вопросам обеспечения информационной безопасности директор ДИББ подчиняется курирующему заместителю председателя правления АО «Узнацбанк».

1.3 Распределение обязанностей между структурными подразделениями ДИББ по обеспечению информационной безопасности следующее:

- УИБ - обеспечение защиты информации, информационных ресурсов и систем АО «Узнацбанк»;
- Управление охраны - обеспечение физической безопасности и режима физического доступа к объектам АО «Узнацбанк».

1.4 Задачи обеспечения информационной безопасности в областных и районных филиалах решаются Отделами по безопасности, режиму и защите информации областных филиалов и главными специалистами по безопасности, режиму и защите информации районных филиалов, которые подчиняются ДИББ и его структурным подразделениям.

1.5 Обязанности по администрированию информационной безопасности в головном офисе АО «Узнацбанк» возлагаются на администратора информационной безопасности АО «Узнацбанк», который является начальником УИБ ДИББ, а в его отсутствие его заместитель.

Обязанности по администрированию информационной безопасности в областных и районных филиалах АО «Узнацбанк» возлагаются сотрудников Отделов по безопасности, режиму и защите информации областных филиалов.

1.6 Обязанности подразделений информационной безопасности и администраторов информационной безопасности определяются настоящей Инструкцией и прописываются в Положениях подразделений и должностных инструкциях.

1.7 Администраторы информационной безопасности АО «Узнацбанк», а также сотрудники подразделений информационной безопасности должны иметь опыт работы в сфере обеспечения информационной безопасности не менее 3-х лет.

1.8 Требования подразделений информационной безопасности и администраторов информационной безопасности, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками АО «Узнацбанк».

1.9 Сотрудники подразделений информационной безопасности и администраторы информационной безопасности в своей деятельности руководствуются:

- Политикой информационной безопасности;
- нормативно-правовыми актами в сфере обеспечения информационной и кибербезопасности;
- приказами и распоряжениями АО «Узнацбанк»;
- актами законодательства, правилами внутреннего трудового распорядка;
- настоящей Инструкцией.

2. Обязанности УИБ ДИББ

2.1 В части обеспечения информационной безопасности УИБ ДИББ и его подразделения должны выполнять следующие обязанности:

1) Отдел анализа и управления информационными рисками (реализация правовых и организационных мер обеспечения информационной безопасности):

- внесение изменений и дополнений в Политику информационной безопасности АО «Узнацбанк»;
- проведение оценки актуализации и эффективности Политики информационной безопасности АО «Узнацбанк» при проведении внутреннего аудита;
- ознакомление сотрудников АО «Узнацбанк» с Политикой информационной безопасности;
- разработка регламентов, корпоративных стандартов и требований, руководств и должностных инструкций (внутренние нормативные документы) по вопросам обеспечения информационной безопасности;
- разработка и внесение на рассмотрение директору ДИББ предложений по совершенствованию внутренних нормативных документов в части обеспечения информационной безопасности;
- доведение внутренних нормативных документов по информационной безопасности до сотрудников АО «Узнацбанк»;
- разработка совместно с подразделениями УИБ ДИББ планов мероприятий по обеспечению информационной безопасности в АО «Узнацбанк»;
- организация и проведение работ по актуализации перечня конфиденциальной информации, реестра информационных активов, категорирование информации и информационных ресурсов АО «Узнацбанк»;
- проведение инвентаризации, определение и ведение перечня объектов защиты, классификация их по уровню защищенности, определение модели угроз в отношении важных и критичных объектов защиты;

- составление и контроль списка сотрудников, получающих доступ к информационным системам и иным объектам защиты;

- ведение учета банкоматов, киосков, электронных платежных терминалов банка;

- закрепление соответствующими организационно-распорядительными документами учетных съемных носителей и накопителей данных за сотрудниками АО «Узнацбанк»;

- ведение учета съемных носителей и накопителей данных, используемых для хранения и передачи конфиденциальной информации в головном офисе АО «Узнацбанк»;

- проведение анализа и оценки рисков информационной безопасности в соответствии с разделом 9 Политики информационной безопасности АО «Узнацбанк»;

- организация и проведение инструктажа (информирование), тренингов и семинаров (обучение) и аттестации(оценка) сотрудников банка по вопросам обеспечения информационной безопасности;

- организация проведения занятий с персоналом АО «Узнацбанк» по ознакомлению и изучению организационно-распорядительных документов обеспечения безопасности информации;

- организация прохождения специалистами АО «Узнацбанк», ответственными за обеспечение информационной безопасности, курсов повышения квалификации;

- оказание методической и практической помощи банковским подразделениям и сотрудникам в вопросах информационной безопасности;

- экспертиза договоров и соглашений АО «Узнацбанк» со сторонними организациями по вопросам обеспечения информационной безопасности при передаче (приеме) информации.

2) Отдел безопасности информационных технологий (обеспечение технической защиты информации):

- выработка требований по обеспечению защиты информации и информационных систем АО «Узнацбанк», а также к организации системы защиты информации в АО «Узнацбанк»;

- планирование и реализация практических мероприятий по внедрению и развитию системы защиты информации;

- определение технических требований к закупаемым средствам технической защиты информации;

- организация закупки средств технической защиты информации в рамках реализации мероприятий по внедрению и развитию системы защиты информации АО «Узнацбанк»;

- проведение организационных мероприятий по подготовке к внедрению и обеспечению эксплуатации системы и средств технической защиты информации, к которым относятся выделение помещения, применение инструкций по эксплуатации и регламентов обслуживания;

- проведение опытно-эксплуатационных и приемно-сдаточных испытаний при внедрении средств технической защиты информации;

- определение сотрудников, ответственных за эксплуатацию

(администрирование) системы защиты и входящих в неё средств технической защиты информации, используемых в АО «Узнацбанк»;

- осуществление управления (администрирование) системой защиты и входящих в неё средств технической защиты информации (межсетевые экраны, прокси-сервера, IDPS, антивирусы, DLP, SIEM, средства анализа и контроля защищенности и др.), включая контроль конфигурации и параметров настройки, восстановление работоспособности, установку обновлений программного обеспечения, корректировку эксплуатационной документации, контроль за событиями безопасности, документирование процедур и результатов контроля;

- обеспечение доступа сотрудников банка к сети Интернет, а также контроль за пользованием ими Интернетом;

- подготовка и внесение директору ДИББ предложений по совершенствованию системы защиты информации в случае выявления недостатков в функционировании и обеспечении защищенности;

- определение и пересмотр порядка установки и модернизации аппаратных и программных средств АО «Узнацбанк» в части обеспечения безопасности информации и процессов ее обработки;

- определение и пересмотр порядка проектирования, разработки, отладки, проверки, внедрения и использования программного обеспечения в части обеспечения безопасности информации и процессов ее обработки;

- организация и проведение внутреннего аудита в части проверки обеспечения мер технической защиты информации, оценки защищенности и выявления уязвимостей и каналов утечек на объектах защиты с применением средств анализа защищенности;

- организация проведения аттестации объектов информатизации АО «Узнацбанк» аккредитованными организациями;

- проведение экспертизы официального веб-сайта АО «Узнацбанк» и иных внешних веб-ресурсов на соответствие требованиям информационной безопасности;

- проведение оценки эффективности принятых технических мер защиты, а также устранение выявленных недостатков по итогам аудитов, экспертиз и аттестаций;

- определение регламента и утверждение графиков проведения профилактических, ремонтных и аварийных работ системы защиты информации и входящих в неё средств технической защиты информации;

- организация и осуществление работ по обнаружению и идентификации инцидентов информационной безопасности, а также ведению их учета;

- организация и координация работ по реагированию на инциденты информационной безопасности, планирование и принятие мер по устранению инцидентов информационной безопасности и их последствий;

- организация и проведение расследований инцидентов информационной безопасности, а также по указанию руководства служебных расследований по фактам нарушения правил обеспечения информационной безопасности;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов информационной безопасности.

- выработка требований по обеспечению криптографической защиты информации в АО «Узнацбанк»;

- планирование и реализация практических мероприятий по внедрению СКЗИ и средств ЭЦП в АО «Узнацбанк»;

- осуществление эксплуатации Центра регистрации ключей ЭЦП и обеспечение его бесперебойного функционирования;

- формирование криптографических ключей шифрования и ЭЦП, сертификатов открытых ключей ЭЦП сотрудникам и клиентам банка;

- регламентирование и обеспечение процессов формирования и выдачи криптографических ключей шифрования и ЭЦП сотрудникам и клиентам банка;

- определение требований и осуществление контроля за обеспечением сохранности криптографических ключей шифрования и ЭЦП сотрудниками банка;

- управление доступом сотрудников банка к ИАБС, а также клиентов банка к банковским услугам Интернет-банкинга и мобильного банкинга путем приостановление и отзыва их сертификатов открытых ключей ЭЦП;

- ведения учета защищенных носителей криптографических ключей шифрования и ЭЦП (token, E-Pass);

- организация и проведение работ по подключению АО «Узнацбанк» к системам денежных переводов;

- выполнение требований подключения операторов денежных переводов АО «Узнацбанк» к системам денежных переводов и управление их доступом;

- подготовка и внесение директору ДИББ предложений по совершенствованию криптографической системы защиты информации в случае выявления недостатков в функционировании и обеспечении защищенности;

- выполнение требований по применению в АО «Узнацбанк» сертифицированных в установленном законодательством Республики Узбекистан порядке СКЗИ;

- организация и проведение внутреннего аудита в части проверки выполнения требований и мер криптографической защиты информации на местах;

- определение регламента и утверждение графиков проведения профилактических, ремонтных и аварийных работ системы криптографической защиты;

- архивация электронных платежей в национальной валюте, проводимых между банками, формирование и проверка состояния электронного архива.

3) Отдел технических средств защиты (оснащение техническими средствами защиты):

- планирование и реализация практических мероприятий по оснащению объектов АО «Узнацбанк» техническими средствами, к которым

относятся СКУД и иные средства контроля доступа в здания и помещения, средства видеонаблюдения, охранной и пожарной сигнализации, средства радиосвязи и др.;

- выработка требований к организации в АО «Узнацбанк» систем видеонаблюдения, охраной и пожарной сигнализации;

- определение технических требований к закупаемым техническим средствам защиты;

- организация закупки технических средств защиты и распределение их по объектам АО «Узнацбанк»;

- организация и контроль выполнения работ, направленных на поддержание работоспособности, модернизацию и совершенствование технических средств защиты;

- проведение экспертизы проектов строящихся и реконструируемых объектов банка на предмет соответствия требованиям безопасности, разработка рекомендаций по оснащению объектов техническими средствами защиты, участие в составе комиссий в приемке материалов и работ, связанных с обеспечением безопасности;

- мониторинг и обсечение работоспособности ведомственной радиосети АО «Узнацбанк», используемой для связи между сотрудниками службы охраны АО «Узнацбанк» с применением мобильных радиостанций;

- взаимодействие с государственными структурами по вопросам организации и порядка работы на средствах радиосвязи в соответствии с действующим законодательством;

- установление требования и осуществление контроля за выдачей, учетом и обеспечением сохранности идентификационных магнитных карт доступа сотрудников банка в служебные помещения;

- проведение проверок по уровню оснащения и применению технических средств защиты, выполнению требований по организации систем видеонаблюдения, охраной и пожарной сигнализации на местах;

3. Обязанности администратора информационной безопасности АО «Узнацбанк»

3.1 В обязанности администратора информационной безопасности АО «Узнацбанк»:

- распределение обязанностей среди специалистов, ответственных за обеспечение информационной безопасности в АО «Узнацбанк» и осуществление контроля за выполнением этими ответственными лицами, закрепленных за ними обязанностей в части обеспечения информационной безопасности;

- определение обязанностей должностных лиц АО «Узнацбанк» по обеспечению безопасности информации, а также привлечение при необходимости иных сотрудников АО «Узнацбанк» в процесс обеспечения информационной безопасности по согласованию с руководством;

- взаимодействие с иными подразделениями АО «Узнацбанк» для обеспечения скоординированных действий по вопросам обеспечения

информационной безопасности;

- обеспечение контроля за выполнением сотрудниками банка положений и требований Политики информационной безопасности АО «Узнацбанк», а также за соблюдением ими требований защиты конкретных систем и выполнения организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- организация и координация работ по выполнению планов мероприятий по обеспечению информационной безопасности в АО «Узнацбанк»;

- контроль за выполнением сетевым администратором корпоративной сети, системным администратором ЛВС АО «Узнацбанк» и администраторами информационной безопасности областных и районных филиалов своих обязанностей в части обеспечения информационной безопасности;

- организация контроля за выполнением специальных требований по размещению технических средств, прокладке кабельных трасс и инженерных систем, за организацией резервного дублирования и архивирования информации, а также созданием и использованием эталонных копий программного обеспечения в части обеспечения безопасности информации и процессов её обработки;

- установление персональной ответственности за эксплуатацию конкретных технических, программных и информационных средств защиты информации.

4. Обязанности Отделов по безопасности, режиму и защите информации областных филиалов

4.1 Задачи Отделов по безопасности, режиму и защите информации в части обеспечения информационной безопасности в областных и районных филиалах и подчиненных им минибанка выполняются администраторами информационной безопасности областных филиалов.

4.2 В обязанности администраторов информационной безопасности областных и районных филиалов входят:

- участие в пересмотре Политики информационной безопасности АО «Узнацбанк» и разработке планов мероприятий по обеспечению защиты информации;

- ознакомление сотрудников областных и районных филиалов Политикой информационной безопасности АО «Узнацбанк» и доведение до них требований внутренних нормативных документов по защите информации;

- контроль за выполнением сотрудниками областных и районных филиалов положений и требований Политики информационной безопасности АО «Узнацбанк», а также за соблюдением ими требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- реализация утвержденных ДИББ планов мероприятий по

обеспечению информационной безопасности в областных и районных филиалах;

- внедрение, эксплуатация и контроль за функционированием средств защиты информации (средства технической защиты, СКЗИ и технические средства защиты) в областных и районных филиалах;

- выполнение требований к организации в областных и районных филиалах систем видеонаблюдения, охраной и пожарной сигнализации;

- проведения профилактических, ремонтных и аварийных работ системы защиты информации в областных и районных филиалах;

- организация и проведение внутреннего аудита информационной безопасности в областных и районных филиалах, выявление уязвимостей и каналов утечек информации;

- контроль состояния обеспечения информационной безопасности и оценка эффективности принятых мер и применяемых средств защиты информации в областных и районных филиалах;

- выявление недостатков в функционировании и обеспечении защищенности, внесение предложений в УИБ ДИББ по совершенствованию системы защиты информации в областных и районных филиалах;

- взаимодействие с УИБ ДИББ и Сектором автоматизации, компьютеризации и внедрения ИКТ для обеспечения скоординированных действий по вопросам обеспечения информационной безопасности в областных и районных филиалах;

- ведение в областных и районных филиалах учета съемных носителей и накопителей данных, используемых для хранения и передачи конфиденциальной информации, защищенных носителей криптографических ключей шифрования и ЭЦП (token, E-Pass) и идентификационных магнитных карт;

- осуществление контроля направления запросов в Центр регистрации ключей ЭЦП на формирование криптографических ключей шифрования и ЭЦП, сертификатов открытых ключей ЭЦП, их приостановление или отзыва (взаимодействие с Центром регистрации ЭЦП по управлению доступом сотрудников и клиентов банка);

- выдача криптографических ключей шифрования и ЭЦП на защищенных носителях (token, E-Pass) сотрудникам областных и районных филиалов, контроль по их защищенному использованию ими;

- контроль за выполнением специальных требований по размещению технических средств, прокладке кабельных трасс и инженерных систем, за резервированием и архивирования информации;

- организация и проведение занятий с персоналом областных и районных филиалов и оказание им методической и практической помощи по вопросам обеспечения информационной безопасности;

- обнаружение, идентификация инцидентов информационной безопасности в областных и районных филиалах;

- своевременное информирование УИБ ДИББ и руководство филиала о возникновении инцидентов информационной безопасности в областных и районных филиалах;

- участие в анализе инцидентов, произошедших в областных и районных филиалах и в расследованиях по ним.

5. Права

5.1 Для решения возложенных обязанностей по обеспечению информационной безопасности УИБ ДИББ имеет следующие права:

- управлять всеми планами по обеспечению информационной безопасности в АО «Узнацбанк»;
- разрабатывать и вносить предложения по изменению Политики информационной безопасности;
- изменять существующие и принимать новые нормативно-методические документы по обеспечению информационной безопасности в АО «Узнацбанк»;
- дополнительно привлекать сотрудников АО «Узнацбанк» в процесс обеспечения информационной безопасности по согласованию с руководством с определением их обязанностей и полномочий;
- контролировать сотрудников банков, в первую очередь сотрудников, имеющих максимальные полномочия, по выполнению требований обеспечения информационной безопасности;
- получать информацию от сотрудников банка по вопросам применения технологий обработки информации и эксплуатации информационных ресурсов и систем;
- рассматривать технические задания и проекты на создание и развитие информационных систем и вносить в них предложения в части обеспечения информационной безопасности;
- участвовать в разработке, тестировании и приемке систем информационной безопасности в информационных системах, практически принимать меры по предотвращению утечки банковских сведений и другой конфиденциальной информации в этих процессах;
- выбирать, внедрять и применять методы, средства и механизмы управления, обеспечения и контроля информационной безопасности банка в пределах своей компетенции;
- организовывать расследования событий, связанных с нарушениями информационной безопасности, вносить предложения руководству по привлечению к ответственности виновных в нарушении требований обеспечения информационной безопасности.

4.2 Отделы по безопасности, режиму и защите информации (администраторы информационной безопасности) областных и районных филиалов имеют следующие права для выполнения своих обязанностей в части обеспечения информационной безопасности:

- вносить предложения по совершенствованию системы защиты в областных и районных филиалах и подчиненных им минибанках;
- контролировать деятельность сотрудников областных и районных филиалов и получать от них информацию по вопросам обеспечения информационной безопасности;

- участвовать в действиях по восстановлению работоспособности после сбоев и аварий в областных и районных филиалах и подчиненных им минибанках;

- контролировать активность, связанную с доступом и использованием средств антивирусной защиты, а также с применением других средств обеспечения информационной безопасности в областных и районных филиалах.

6. Ответственность

4.5 Начальники и сотрудники подразделений информационной безопасности АО «Узнацбанк», администраторы информационной безопасности областных филиалов несут ответственность за:

- неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных настоящей Инструкцией;

- качество проводимых им работ по обеспечению информационной безопасности в АО «Узнацбанк»;

- состояние и поддержание установленного уровня защиты сетей, информационных ресурсов и систем АО «Узнацбанк».

Приложение №6
к Политике информационной
безопасности АО «Узнацбанк»
№124-б от 27.12.2021г

Положение по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных

1. Общие положения

1.1 Настоящее Положение по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных определяет:

- порядок обновления системного и прикладного программного обеспечения, внесения в них изменений и модификации;
- порядок резервного копирования и архивирования данных для последующего восстановления работоспособности информационных систем или её частей при полной или частичной потере информации, вызванной сбоями или отказами оборудования, нарушениями информационной безопасности, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- обязанности лиц, занимающихся резервированием данных и обновлением программного обеспечения.

1.2 В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- обновление, внесение изменений и модификации программного обеспечения.

1.3 Целью резервного копирования является предотвращение потери информации при сбоях оборудования и программного обеспечения, в критических ситуациях.

1.4 Настоящее Положение распространяется на системное и прикладное программное обеспечение, а также данные, используемые в АО «Узнацбанк».

2. Задачи по установке, внесению изменений, конфигурированию и обновлению программного обеспечения

2.1 В задачи по установке, внесению изменений, конфигурированию и обновлению программного обеспечения входят:

- установка вновь разработанного, измененного или приобретенного программного обеспечения;
- настройка (конфигурация) программного обеспечения; внесение изменений в настройку (конфигурацию) программного обеспечения;

- внесение изменений в исходный код программного обеспечения в случае потребности изменений определенных задач и функций программы или информационной системы;

- тестирование вновь разработанного программного обеспечения или измененного программного обеспечения перед установкой на действующем оборудовании (вводом в эксплуатацию);

- отслеживание обновлений программного обеспечения от производителей (разработчиков);

- обновление программного обеспечения;

- проверка правильности функционирования программного обеспечения после её установки и настройки, внесения изменений в настройки и обновления программного обеспечения.

2.2 Задачи по внесению изменений, конфигурированию и обновлению программного обеспечения возлагаются на:

- системного администратора ЛВС АО «Узнацбанк» - операционная система сервера ЛВС АО «Узнацбанк»;

- сотрудников Отдела системного программного обеспечения ДИТ – операционная система и программное обеспечение сервера корпоративной электронной почты, операционная система и программы рабочих станций головного офиса;

- сотрудников Сектора автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов – операционные системы и программы серверов и рабочих станций областных и районных филиалов, подчиненных им минибанков;

- сетевого администратора корпоративной сети и сотрудников Отдела сопровождения сетевой инфраструктуры ДИТ – программное обеспечение сетевого оборудования головного офиса, коммутаторов ядра сети и маршрутизаторов, серверов видеоконференцсвязи и IP-телефонии;

- сотрудников УИБ ДИББ – программное обеспечение обслуживаемых ими межсетевых экранов и средств IDPS, средств антивирусной защиты, системы SIEM, СКЗИ и других средств защиты информации, операционная система и прикладная программа Центра регистрации ключей ЭЦП;

- администраторов информационной безопасности областных и районных филиалов – программное обеспечение средств антивирусной защиты областных и районных филиалов;

- системные администраторы информационных систем и сотрудники Управления поддержки информационных систем и Отдела системного программного обеспечения ДИТ – операционные системы и СУБД сервера базы данных, операционные системы и приложения серверов приложений, прикладное программное обеспечение информационных систем (ИАБ, БИС, система электронного документооборота, процессингового сервера SWIFT);

- сотрудники ДРБ –операционные системы и СУБД сервера базы данных, операционные системы и приложения серверов приложений, прикладное программное обеспечение системы процессинга VISA/MasterCardAO «Узнацбанк».

2.3 Установка программного обеспечения производится:

- при вводе информационной системы или средств в эксплуатацию;

- на основании заявки подразделений АО «Узнацбанк»;

- в случае замены, установки нового или переустановки действующего устройства.

2.4 Изменения и обновления программного обеспечения производятся в случаях:

- появления новой версии или обновлений от производителя (разработчика) программного обеспечения;

- необходимости устранения выявленных уязвимостей или ошибок в программном обеспечении;

- потребности изменений задач и функций программного обеспечения».

2.5 Все изменения и обновления программного обеспечения должны строго контролироваться указанными сотрудниками, для каждой операции подготавливаются процедуры тестирования.

2.6 Для изменений и обновлений в программное обеспечение, которые производителем или разработчиком квалифицируются как важные или критические, необходимо инициировать процедуру применения этого исправления вне очереди. Решения о необходимости применения важных и критических настроек или обновлений принимается руководителями ДИТ, ДИББ и ДРБ в течение 3 (трех) суток с момента поступления и уведомления. В случае отказа от установки таких обновлений должны быть приняты адекватные меры по устранению выявленных уязвимостей или ошибок, которые ликвидировались отклоненным обновлением.

2.7 Источником информации о выходе обновлений прикладного и системного программного обеспечения могут быть почтовые рассылки от разработчика программного обеспечения, профильные интернет-сайты. Другим источником информации об отсутствующих обновлениях могут быть результаты работы системы обнаружения и управления уязвимостями, результаты работы сканеров безопасности.

2.8 Обязательному обновлению подлежат следующее программное обеспечением:

- операционные системы сервера ЛВС АО «Узнацбанк», серверов баз данных и серверов приложений информационных систем, сервера Центра регистрации ключей ЭЦП, сервера корпоративной электронной почты;

- СУБД серверов баз данных информационных систем и Центра регистрации ключей ЭЦП;

- веб-приложения серверов приложений информационных систем;

- программное обеспечение средств защиты информации и операционных систем серверов централизованных систем антивирусной защиты.

2.9 Решение о необходимости обновления, указанного в пункте 2.4 программного обеспечения, производится по решению директоров ДИТ, ДИББ и ДРБ. Данные обновления должны производиться в нерабочее время с перегрузкой серверов. После обновления должны быть произведены все проверки и тестирования для оценки нормального функционирования

серверов, обновленного программного обеспечения, установленных на них прикладного программного обеспечения и сохранность данных.

2.10 Внесение изменений в прикладное программное обеспечение производится в случае модификации её разработчиком, потребностью или необходимостью АО «Узнацбанк» во внесении изменений в функционал или в дальнейшем развитии информационных систем.

Для информационных систем ИАБС, БИС, система электронного документооборота и Центра регистрации ключей ЭЦП должны выполняться следующие требования по модификации и внесению изменений в их прикладное программное обеспечение:

- модифицированное или измененное прикладное программное обеспечение должно пройти тестирование на отдельных тестовых серверах с проверкой выполнения всех действующих и новых функций информационной системы;
- установка проверенного модифицированного или измененного прикладного программного обеспечения в нерабочее время после полной их проверки;
- обеспечение сохранности всей информации в базе данных информационных системы при установке модифицированного или измененного прикладного программного обеспечения;
- проведение после установки всех проверок и тестирований для оценки нормального функционирования серверов, установленных на них модифицированного или измененного прикладного программного обеспечения и сохранность данных информационной системы.

3. Ответственность за обновление системного и прикладного программного обеспечения

3.1 Ответственность за обновление системного и прикладного программного обеспечения возлагается на сотрудников, указанных в пункте 2.1 настоящего Положения.

3.2 Контроль за выполнением требований по обновлению системного и прикладного программного обеспечения со стороны обслуживающих сотрудников осуществляется ДИТ, ДИББ, ДРБ.

4. Классификация типов резервного копирования

4.1 По типу резервируемая информация делится:
- операционные системы и утилиты;
- прикладное (специализированное) программное обеспечение;
- данные.

4.2 Места хранения резервной информации:
- сервера;
- рабочие станции;
- свободные жесткие диски или свободное пространство жестких дисков;

- съемные носители.

4.3 Методы резервного копирования:

- клонирование (point-in-time), т.е. создание нескольких физических копий томов (клонов);

- создание мгновенной копии (snapshot), т.е. создание логической копии диска, его образа;

- копирование.

По полноте сохраняемой информации:

- полное резервирование (Full backup) — создание резервной копии всех подлежащих резервированию данных, необходимых для полного восстановления технологического оборудования;

- добавочное резервирование (Incremental backup) — создание резервной копии всех данных, которые были модифицированы после предыдущего полного или добавочного резервирования;

- разностное резервирование (Differential backup) — создание резервной копии всех данных, которые были изменены после предыдущего полного резервирования.

4.4 По способу доступа к носителю:

- оперативное резервирование (Online backup) — создание резервного архива на постоянно подключенном (напрямую или через сеть) носителе;

- автономное резервирование (Offline backup) — хранение резервной копии на съёмном носителе, кассете или картридже, который перед использованием следует установить в привод.

4.5 По времени выполнения резервной копии:

- резервные копии реального времени — данные резервируются непосредственно при их появлении в системе — при помощи репликации, распределенных хранилищ и т.п.

- плановые резервные копии — данные резервируются в определенные заранее моменты времени.

5. Порядок резервного копирования

5.1 Резервное копирование информации производится на основании следующих данных: состав и объем копируемых данных, периодичность проведения резервного копирования и срок хранения копий.

5.2 Система резервного копирования должна обеспечивать производительность, достаточную для сохранения важной информации.

Для исключения человеческого фактора и минимизации ущерба, связанного с восстановлением некорректных данных, система резервного копирования и восстановления должна быть автоматизирована с учетом минимального вмешательства контролирующего персонала.

5.3 Ответственный за резервное копирование должен обеспечивать:

- первоначальную настройку системы резервного копирования (создание расписаний, оповещений и пр.), запуск в эксплуатацию системы резервного копирования;

- внесение существенных изменений в настройку системы резервного копирования;

- анализ журнала резервного копирования, отслеживание необходимости изменений настроек резервного копирования;

- контроль резервного копирования или оборудования;

- контроль результатов резервного копирования;

- выполнение порядка и условий хранения носителей информации, содержащих резервные копии;

- восстановление данных с резервных копий.

5.4 Для ИАБС должен создаваться электронный архив в соответствии с требованиями Положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан, утвержденного постановлением Правления Центрального банка Республики Узбекистан от 25 января 2020 года №2/4.

6. Перечень резервируемой информации

6.1 Резервному копированию подлежат данные, необходимые для восстановления работоспособности информационных систем, операционные системы, прикладное программное обеспечение, конфигурация системы.

Перечень резервируемой информации АО «Узнацбанк», а также ответственные за резервное копирование приведены в таблице №1.

6.2. В перечень резервируемой информации могут вноситься изменения и дополнения по мере появления новых информационных систем и средств. Изменения и дополнения в данный перечень вносится ДИТ, ДИББ и ДРБ.

6.3 Дополнительно отдельные информационные ресурсы подлежать электронному архивированию. Электронный архив должен включать следующие информационные ресурсы:

- полная электронная база данных дня банковской практики;

- открытые ключи с истекшим сроком действия и ключи ЭЦП;

- дневные программы банковской практики и набор других программ, используемых в отдельном банке;

- электронные протоколы, связанные с электронными платежными системами, программными и программно-аппаратными сетевыми устройствами, а также инциденты информационной безопасности;

- документы, связанные с платежами, полученными и переданными по электронной почте (приказы, решения и т. д.);

- все входящие и исходящие электронные платежные документы в зашифрованном и незашифрованном виде;

- информация коммерческих банков о кредитных и других банковских операциях;

- информация о системе управления банками.

Таблица №1. Перечень резервируемой информации АО «Узнацбанк»

№	Резервируемая информация	Способ резервирования	Периодичность создания резервной копии	Ответственный
1.	**Интегрированная Автоматизированная Банковская система (ИАБС)**			
1.1.	База данных ИАБС, журналы	Создание резервной копии в системе хранения данных основного ЦОД с использованием технологии RAID, а также репликация данных с системы хранения данных основного ЦОД на систему хранения данных резервного ЦОД (физически отдельные дисковые массивы основного и резервного ЦОД)	Автоматически, постоянно производится резервирование и репликация данных	Системный администратор ИАБС (Управление поддержки информационных систем ДИТ)
1.2.	Электронный архив ИАБС	Сохранение электронного архива на отдельные носители (картриджи)	Ежедневно, в конце операционного дня, вручную	
1.3.	Операционная система серверов базы данных и приложений	Дублирование операционной системы на физических отдельных серверах базы данных в основном и резервном ЦОД. Дублирование операционной системы серверов приложений на основном физическом сервере и резервном виртуальном сервере. Создание образа операционной системы сервера базы данных и серверов приложений и хранение их на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы, а также после каждого её обновления	

1.4.	Веб-приложение серверов приложений	Дублирование веб-приложений серверов приложений на основном физическом сервере и резервном виртуальном сервере	Вручную после первоначальной установки или переустановки веб-приложения, а также после каждого её обновления	
1.5.	Прикладная программа ИАБС	Дублирование прикладной программы на физических отдельных серверах базы данных в основном и резервном ЦОД. Создание резервной копии.	Вручную после установки прикладной программы и после каждого её обновления создается копия.	
2.	**Банковская информационная система (БИС)**			
2.1.	База данных БИС, журналы	Создание резервной копии в системе хранения данных основного ЦОД с использованием технологии RAID, а также копирование (полный backup) данных на отдельные носители	Автоматически, постоянно производится резервирование Каждую неделю в выходные копирование данных на отдельные носители, вручную	Системный администратор БИС (Управление поддержки информационных систем ДИТ)
2.2.	Электронный архив ИАБС	Сохранение электронного архива на отдельные накопители (магнитные ленты)	Ежедневно, в конце операционного дня, вручную	
2.3.	Операционная система сервера базы данных и приложений	Дублирование операционной системы сервера базы данных и сервера приложений на основном физическом сервере и резервном виртуальном сервере. Создание образа операционной системы сервера базы данных и сервера приложений и хранение их на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы, а также после каждого её обновления	
2.4.	Веб-приложение сервера приложений	Дублирование веб-приложений сервера приложений на основном	Вручную после первоначальной установки или переустановки	

		физическом сервере и резервном виртуальном сервере	веб-приложения, а также после каждого её обновления	
2.5.	Прикладная программа БИС	Дублирование прикладной программы на физическом отдельном сервере базы данных и виртуальном резервном сервере. Создание резервной копии.	Вручную после установки прикладной программы и после каждого её обновления создается копия.	
3.	**Система электронного документооборота АО «Узнацбанк»**			
3.1.	База данных СЭД, журналы	Создание резервной копии в системе хранения данных на сервере СЭД с использованием технологии RAID, а также копирование (полный backup) данных на отдельные носители	Автоматически, постоянно производится резервирование Каждую неделю в выходные копирование данных на отдельные носители	Системный администратор СЭД (Отдел системного программного обеспечения ДИТ)
3.2.	Операционная система сервера СЭД	Дублирование операционной системы на основном физическом сервере и резервном виртуальном сервере ЭДО. Создание образа операционной системы сервера СЭД и хранение его на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы, а также после каждого её обновления	
3.3.	Прикладная программа СЭД	Дублирование прикладной программы на физическом отдельном сервере СЭД и виртуальном резервном сервере СЭД. Создание резервной копии	Вручную после установки прикладной программы и после каждого её обновления создается её копия	
4.	**Центр регистрации ключей ЭЦП АО «Узнацбанк»**			
4.1.	База данных ЦРК ЭЦП, журналы	Создание резервной копии в системе хранения данных на сервере ЦРК ЭЦП с использованием технологии RAID,	Автоматически, постоянно производится резервирование	Администратор ЦРК ЭЦП (УИБ ДИББ)

		а также копирование (полный backup) данных на отдельные носители.	Каждую неделю в выходные копирование данных на отдельные носители	
4.2.	Операционная система сервера ЦРК ЭЦП	Создание образа операционной системы сервера ЦРК ЭЦП и хранение его на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы, а также после каждого её обновления	
4.3.	Прикладная программа СЭД	Создание резервной копии	Вручную после установки прикладной программы и после каждого её обновления создается копия	
5.	**Процессинговый сервер SWIFT**			
5.1.	База данных сервера SWIFT	Копирование (полный backup) базы данных на отдельные носители (магнитные ленты)	Вручную или с помощью скриптов, ежедневно в конце операционного дня	Системный администратор SWIFT (Отдел системного программного обеспечения ДИТ)
5.1.	Операционная система и программное обеспечение сервера SWIFT	Дублирование операционной системы и программного обеспечения на физически отдельных основном и резервном сервере. Создание образа операционной системы сервера SWIFT и хранение его на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы и/или программного обеспечения, а также после каждого её обновления	
6.	**Процессинговый сервер VISA/MasterCard**			
6.1.	База данных сервера VISA/MasterCard	Копирование (полный backup) базы данных на отдельные носители (магнитные ленты)	Вручную, ежедневно в конце операционного дня	Системный администратор VISA/MasterCard

6.1.	Операционная система и программное обеспечение сервера VISA/MasterCard	Дублирование операционной системы и программного обеспечения на физически отдельных основном и резервном сервере. Создание образа операционной системы сервера VISA/MasterCard и хранение его на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы и/или программного обеспечения, а также после каждого её обновления	(ДРБ)
7.	**Файловый FTP сервер головного офиса и областных филиалов**			
7.1.	Файлы FTP сервера	Копирование файлов на отдельный жесткий диск сервера	По графику	Системный администратор ЛВС АО «Узнацбанк», сотрудники Сектора автоматизации, компьютеризации и внедрения ИКТ областных филиалов
7.2.	Операционная система FTP сервера	Создание образа операционной системы FTP сервера и хранение его на отдельном жестком диске	Вручную после первоначальной установки или переустановки операционной системы, а также после каждого её обновления	
8.	**Почтовый сервер корпоративной электронной почты**			
8.1.	Почтовый сервер	Резервное копирование данных через VEEAM на отдельный носитель	Ежедневно, вручную	Системный администратор ЛВС АО «Узнацбанк»
9.	**Сервера антивируса**			
9.1.	Конфигурируемые параметры (настройки)	Копирование файлов на отдельный жесткий диск сервера	Ежегодно, а также при изменении параметров настроек	Сотрудник УИБ ДИББ и администратор информационной безопасности областного филиала
10.	**Межсетевые экраны и средства IDPS, прокси-сервера**			

10.1.	Конфигурируемые параметры (настройки)	Копирование файлов на отдельный жесткий диск сервера	Ежегодно, а также при изменении параметров настроек	Сотрудники УИБ ДИББ
11.	**Основное сетевое оборудование**			
11.1.	Конфигурируемые параметры (настройки) коммутаторы ядра корпоративной сети	Копирование файлов на отдельный жесткий диск или съемный носитель	Ежегодно, а также при изменении параметров настроек	Сетевой администратор корпоративной сети (Отдел сопровождения сетевой инфраструктуры ДИТ)

7. 7. Порядок и условия учета, хранения и списания носителей информации, содержащих резервные копии

7.1 Носителям информации, содержащим резервную копию и/или электронный архив, присваивается уровень конфиденциальности по наивысшему уровню конфиденциальности содержащихся в них сведений.

7.2 Носители резервных копий должны быгь учтены и промаркированы (дата копирования, наименование ресурса, срок хранения, количество копий, номер тома и т.п.).

Учет носителей резервных копий ведется сотрудниками ДИТ, ДИББ и ДРБ, указанных в таблице №1 настоящего Положения, в соответствии с Инструкцией по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных, приведенной в приложении №9 к Политике информационной безопасности АО «Узнацбанк».

Носители резервных копий маркируются, как информационные активы в соответствии с требованиями Порядка управления информационными активами, приведенным в приложении №13 к Политике информационной безопасности АО «Узнацбанк». Ответсвеность за маркирование резервных копий лежит на сотрудников ДИТ, ДИББ и ДРБ, указанных в таблице №1 настоящего Положения.

7.3 Хранение резервных копий должно осуществляться в отдельных помещениях максимально удаленных от основных серверных помещений, оборудованных системами пожаротушения и предотвращения несанкционированного доступа.

7.4 Электронный архив информационных ресурсов следует скопировать на внешнее хранилище и хранить в сейфе или металлическом шкафу.

7.5 В случае выхода из строя системы резервного копирования должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, систем хранении данных, располагающих необходимыми объемами дискового пространства для ее хранения.

7.6 В случае недоступности системы резервного копирования, резервирование должно осущсствляться на виртуальный сервер резервного копирования.

7.7 Списание и уничтожение носителей резервных копий осуществляется в соответствии с Инструкцией по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных, приведенной в приложении №9 к Политике информационной безопасности АО «Узнацбанк».

8. Контроль результатов резервного копирования

8.1 Контроль результатов всех процедур резервного копирования осуществляется лицами, ответственными за резервное копирование, которые указаны в таблице №1настоящего Положения.

8.2 Контроль результатов процедур резервного копирования производится сразу после создании копии.

8.3 Контроль результатов процедур резервного копирования баз данных информационных систем АО «Узнацбанк» осуществляется системами резервного копирования и восстановления:

- Veem для систем: ИАБС, БИС, СЭД, база данных сервера VISA/MasterCard, корпоративная электронная почта;
- Acronis – база данных Центр регистрации ключей ЭЦП;
- AIX - база данных сервера SWIFT.

8.4 При контроле результатов резервного копирования проверяется:

- правильность выполнения всех процедур копирования, т.е. отсутствие ошибок при копировании;
- перечень скопированных данных, файлов, каталогов;
- соответствие объема скопированных файлов к объему, подлежащему копированию (архивированию);
- проверка на отсутствии вредоносных программ антивирусными средствами.

Указанные процедуры контроля результатов резервного копирования осуществляются ответственным лицом и/или системой резервного копирования и восстановления данных под контролем ответственного лица.

8.5 В случае обнаружения ошибки лицо, ответственное за контроль результатов резервного копирования, сообщает директору ДИТ, ДИББ и ДРБ.

8.6 При обнаружении ошибок резервного копирования проводится повторная процедура копирования. При повторном возникновении ошибок выясняются причины: неисправность или неправильная настройка системы резервного копирования, переполненность или неисправность резервного носителя и др. и принимаются меры по их устранению.

9. Порядок восстановления информации

9.1 Восстановление данных из резервных копий производится в случае потери работоспособности информационной системы или её компонента и выполняется на основании разрешения директора ДИТ, ДИББ и ДРБ.

9.2 В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагавшийся к системе резервного копирования, и документации разработчика прикладного программного обеспечения информационной системы.

9.3 Восстановление данных осуществляется в максимально сжатые сроки, указанные в Плане восстановления функционирования информационных систем.

9.4 Процедура проверки восстановления резервированных данных производится сразу после их восстановления.

9.5 При проверке резервированных данных после восстановления осуществляется:

- проверка правильности выполнения всех процедур восстановления, т.е. перечень выполненных процедур и отсутствие ошибок при их выполнении;
- перечень скопированных данных, файлов, каталогов;
- соответствие объема восстановленных файлов, т.е. оценивается целостность данных посредством поочередного открытия файлов в соответствующих приложениях;
- проверка отсутствия вредоносных программ в восстановленных данных антивирусными средствами.

Указанные процедуры проверки правильности восстановления резервированных данных осуществляются ответственным лицом и/или системой резервного копирования и восстановления данных под контролем ответственного лица.

9.6 В случае обнаружения ошибки лицо, ответственное за проверку восстановления резервированных данных, сообщает директору ДИТ, ДИББ и ДРБ.

9.7 При обнаружении ошибок восстановления резервированных данных проводится повторная процедура восстановления. При повторном возникновении ошибок выясняются причины: неисправность или неправильная настройка системы резервного копирования, переполненность или неисправность носителя и др. и принимаются меры по их устранению.

Приложение №7
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 от 27.12.2021г

Инструкция по парольной защите и аутентификации

1. Общие положения

1.1 Настоящая Инструкция определяет порядок, правила формирования и использования, а также требования к парольной защите и аутентификации при доступе к объектам информатизации АО «Узнацбанк».

1.2 Настоящая Инструкция распространяется на сотрудников, формирующих и управляющих парольной защитой и иными идентификаторами доступа к объектам информатизации, а также распространяется на всех сотрудников АО «Узнацбанк», осуществляющих доступ к этим объектам.

1.3 Доступ сотрудников к информационным ресурсам и системам АО «Узнацбанк» должен разграничиваться в соответствии с Матрицей доступа к информационным ресурсам (далее - Матрица), которая разрабатывается в соответствии с Правилами по разработке матрицы доступа к информационным ресурсам, приведенными в приложении №10 к Политике информационной безопасности АО «Узнацбанк».

2. Термины и определения

2.1 В настоящей Инструкции применены следующие термины и их определения:

авторизация: предоставление права определенному лицу или группе лиц совершать определенные действия;

аутентификация: процедура установления подлинности пользователя, программы, устройства или данных;

идентификация: присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

инициализационный пароль - пароль, выдаваемый пользователю для первоначального входа в систему;

компрометация пароля - известность пароля или принципа его формирования посторонним лицам;

криптографический ключ - последовательность секретных символов, которые выполняют шифрование, дешифрование, формирование и проверку электронных подписей с использованием криптографических алгоритмов;

парольная защита - управление процессом доступа к системе, ее ресурсам посредством паролей;

пароль - секретный набор символов, используемый для аутентификации пользователя;

учетная запись - идентификатор пользователя, используемый для доступа к информационным системам и ресурсам.

3. Общие требования

3.1 Парольная защита и аутентификация должна использоваться при обеспечении доступа сотрудников АО «Узнацбанк» к следующим объектам информатизации:

1) однофакторная аутентификация на основе идентификационной магнитной карты:

- защищаемым помещениям 2 и 3-зоны, включая серверные помещения ЦОД, коммутационные помещения областных и районных филиалов;

2) однофакторная аутентификация на основе логина и пароля при доступе к:

- рабочим станциям, ЛВС АО «Узнацбанк» и корпоративной сети – сотрудниками АО «Узнацбанк»;
- серверному оборудованию – администраторами (обслуживающими сотрудниками);
- сетевому оборудованию – администраторами (обслуживающими сотрудниками);
- средствам защиты информации – администраторами (обслуживающими сотрудниками);
- БИС - сотрудниками АО «Узнацбанк» и системным администратором;
- системе электронного документооборота - сотрудниками АО «Узнацбанк» и администратором системы;

3) двухфакторная аутентификация на основе логина и пароля, а также ЭЦП, формируемого криптографическим ключом, при доступе к:

- системам защищенной электронной почты E-xat и контроля исполнительской дисциплины E-ijro – сотрудниками АО «Узнацбанк»;
- Интернет-банкингу и мобильному банкингу – клиентами банка при пользовании интерактивными банковскими услугами (для клиентов мобильного банкинга дополнительно используется аутентификация по SMS-коду при регистрации клиента к мобильному приложению);
- Центру регистрации ключей ЭЦП АО «Узнацбанк» - администратором центра;
- международным системам денежных переводов – сотрудники банка (операторы денежных переводов) и администратор систем;

4) трехфакторная аутентификация на основе логина и пароля, носителя ключевой информации, а также ЭЦП, формируемого закрытым ключом ЭЦП, при доступе к ИАБС - сотрудники АО «Узнацбанк» и администратором.

3.2 Для проверки ЭЦП при доступе сотрудников к ИАБС и клиентов АО «Узнацбанк» к банковским услугам используются сертификаты открытого ключа ЭЦП, хранящиеся Центре регистрации ключей ЭЦП АО «Узнацбанк».

3.3 Центр регистрации ключей ЭЦП АО «Узнацбанк» осуществляется деятельность (функции, права и обязанности) в соответствии с Положением о

порядке работы Центра регистрации ЭЦП АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

3.4 При формирование закрытых ключей ЭЦП и сертификатов открытых ключей ЭЦП Центр регистрации ключей ЭЦП АО «Узнацбанк» руководствуется государственными стандартами O‘Z DSt 081: 1092:2009 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и O‘ZDSt 081 1108:2011 «Информационная технология. Взаимосвязь открытых систем. Структура сертификата открытого ключа ЭЦП и сертификата атрибута».

3.5 Пароли, магнитные идентификационные карты и криптографические ключи являются конфиденциальной информацией и не могут быть разглашены, либо переданы кому-либо. Ответственность за безопасное хранение пароля и криптографического ключа лежит на их владельце.

3.6 Рабочие станции должны быть настроены на автоматическое блокирование в случае отсутствия активности сотрудника банка в течение 10 минут, и переход в спящий режим - 30 минут, гибернация - 60 минут. Разблокировка должна производиться после повторного ввода пароля.

4. Требования обеспечения сохранности паролей и иных идентификаторов

4.1 Сотрудники банка несут персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.

4.2 Хранение сотрудником банка значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе системного администратора или руководителя подразделения АО «Узнацбанк» в опечатанном печатью пенале.

4.3 В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, работ, проводимых ДИТ или Сектором автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных или проверочных работ сотрудники банка самостоятельно производят немедленную смену значений «раскрытых» паролей.

4.4 В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей пользователей (в их отсутствие) допускается изменение паролей системным администратором АО «Узнацбанк». В подобных случаях, сотрудники банка, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения.

4.5 В случае длительного отсутствия сотрудника банка (командировка, болезнь и т.п.) его учетная запись блокируется) и, в случае необходимости,

изменяются права доступа других пользователей в отношении ресурсов данного сотрудника.

4.6 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, несоответствующих данным требованиям, а также за разглашение парольной информации.

4.7 Пароли встроенных административных учетных записей серверов, сетевого оборудования и средств защиты информации должны храниться в защищенном месте в несгораемом сейфе. Доступ к этим паролям возможен только с санкции начальников подразделений ДИТ, ДРБ и ДИББ, а в областных и районных филиалах начальников Отделов по безопасности, режиму и защите информации и начальников Секторов автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов.

4.8 Сотрудники банка несут персональную ответственность за сохранность идентификационных магнитных карт, используемые для доступа в защищаемым помещениям 2 и 3-зоны, включая серверные помещения ЦОД, коммутационные помещения областных и районных филиалов АО «Узнацбанк».

Идентификационные магнитные карты не должны передавать иным сотрудникам банка, в особенности, сторонним лицам.

4.9 Доступ сотрудников АО «Узнацбанк» к ИАБС осуществляется на основе ЭЦП, формируемой закрытым ключом ЭЦП, принадлежащим сотруднику банка. Закрытые ключи ЭЦП и сертификаты открытых ключей ЭЦП выдаются сотруднику банка на защищенном носителе token.

Также закрытые ключи ЭЦП и сертификаты открытых ключей ЭЦП выдаются клиентам Интернет-банкинга и мобильного банкинга для пользования интерактивными банковскими услугами АО «Узнацбанк». Указанные ключи выдаются клиентам банка на носителе E-Pass.

4.10 Защищенное хранение закрытого ключа ЭЦП обеспечивается самим сотрудником АО «Узнацбанк» и клиентами банка.

Доступ к закрытому ключу ЭЦП осуществляется по паролю его владельца, который известен только ему. Сотрудники АО «Узнацбанк» должны использовать сложные пароли для доступа к ключу ЭЦП в соответствии с требованиями, определенными в разделе 7 настоящей Инструкции.

4.11 Сотрудники АО «Узнацбанк» и клиенты банка должны выполнять требования по обеспечению сохранности носителей ключевой информации, которые определены в заявке сотрудника АО «Узнацбанк» на выдачу ключей и сертификатов открытых ключей ЭЦП, а для клиентов банка – в договорах на оказание услуг.

5. Организационно-техническое обеспечение процессов генерации паролей, закрытых ключей ЭЦП и сертификатов открытых ключей ЭЦП

5.1 Для доступа новых сотрудников АО «Узнацбанк» к рабочим станциям (ЛВС АО «Узнацбанк» и корпоративной сети) формируется новая учетная запись (логин) и инициализационный пароль.

Указанные учетные данные (логин) и инициализационный пароль формируется Отделом системного программного обеспечения ДИТ и выдается новому сотруднику.

5.2 Для доступа новых сотрудников к информационным системам АО «Узнацбанк» формируется логин и инициализационный пароль системными администраторами данных информационных систем.

5.3 Клиенты банка для доступа к Интернет-банкингу и мобильному банкингу формируют логин и пароль сами при регистрации в банковской системе.

5.4 В качестве технического обеспечения процессов генерации инициализированных паролей для сотрудников АО «Узнацбанк» используются генераторы паролей.

5.5 Инициализированный пароль доступа к рабочим станциям (ЛВС, корпоративной сети) предоставляется новому сотруднику АО «Узнацбанк» по корпоративной электронной почте или нарочно.

Инициализированный пароль доступа к информационным системам предоставляется сотруднику АО «Узнацбанк» только нарочно или по служебной почте.

5.6 После доступа по инициализационному паролю новый сотрудник обязан ввести свой пароль с выполнением требований и правил формирования паролей, определенных в разделе 7 настоящей Инструкции.

5.7 Для ограничения доступа посторонних лиц к серверному, сетевому оборудованию и средствам защиты информации пароли доступа к ним, а также к рабочим станциям, обеспечивающим удаленный доступ к ним, формируются и используются сотрудниками, ответственными за их эксплуатацию – администраторами.

5.8 Для формирования закрытых ключей ЭЦП для сотрудников банка и клиентов банка должны направляться запросы в Центр регистрации ключей ЭЦП.

5.9 Запросы в Центр регистрации ключей ЭЦП на формирование криптографических закрытых и открытых ключей ЭЦП для клиентов Интернет-банкинга, а также ответственным сотрудникам банка имеющих доступ к системе ИАБС возлагается на сотрудников Сектора автоматизации и компьютеризации областных филиалов и Главного специалиста по автоматизации районных филиалов при контроле Отдела по безопасности, режиму и защите информации областных филиалов, на основании заявления клиентов и сотрудников банка, форма которой приведена в Положении о порядке работы Центра регистрации ЭЦП АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

5.10 Криптографические закрытые ключи ЭЦП, используемые для формирования ЭЦП при доступе сотрудников к ИАБС и клиентов к интерактивным банковским услугам, генерируются и сертификаты открытых ключей ЭЦП формируются ответственным сотрудником УИБ ДИББ, являющийся администратором Центра регистрации ключей ЭЦП АО «Узнацбанк».

5.11 Генерация закрытого ключа ЭЦП и формирование открытого ключа ЭЦП обеспечивается программным обеспечением Центра регистрации ключей ЭЦП АО «Узнацбанк».

5.12 Созданные криптографические закрытые ключи ЭЦП записываются на защищенный USB-носитель (token).

5.13 Криптографические ключи на защищенном носителе выдаются сотрудникам банка ответственными сотрудниками информационной безопасности УИБ, в районных филиалах под роспись в специальном журнале, в котором указывается:

- Ф.И.О и должность сотрудника;
- серийный номер носителя ключевой информации;
- дата и время выдачи.

5.14 Криптографические ключи на защищенном USB-носителе выдаются клиентам банка для работы в Интернет-банкинге ответственными сотрудниками областных и районных филиалов.

5.15 До выдачи криптографических ключей на защищенном носителе, они должны храниться в сейфе подразделений информационной безопасности.

5.16 Сертификаты открытых ключей ЭЦП заносятся в базу Центра регистрации ключей ЭЦП АО «Узнацбанк».

Управление доступом к ИАБС с применением ЭЦП осуществляется путем приостановления действия и отзыва сертификата открытых ключей ЭЦП в базе Центра регистрации ключей ЭЦП АО «Узнацбанк» его администратором.

6. Процессы смены и прекращения действия паролей и иных идентификаторов

6.1 Сотрудники АО «Узнацбанк» при доступе к рабочим станциям (ЛВС и корпоративной сети АО «Узнацбанк») должны сменять свой пароль не реже одного раза в течение 3-х месяцев. Данное требование должно обеспечиваться путем соответствующих настроек службы Active Directory Windows Server сервера ЛВС АО «Узнацбанк» по управлению учетными записями.

6.2 Сотрудники банка и клиенты банка при доступе к информационным системам АО «Узнацбанк» должны сменять свой пароль не реже одного раза в течение 3-х месяцев. В ИАБС смена пароля сотрудника банка должна производиться не менее 1 раза в месяц.

Данное требование должно обеспечиваться путем соответствующих настроек в системе управления доступом пользователей в информационных системах.

6.3 В системе электронного документооборота АО «Узнацбанк» смена пароля сотрудника банка производится самим пользователем самостоятельно, не реже одного раза в год.

6.4 В настройках службы Active Directory Windows Server и систем управления доступом пользователей в информационных системах должны выполняться следующие требования смены пароля сотрудниками банка:

- периодическая смена пароля самим пользователем;
- сложность вводимого пароля в соответствии с требованиями раздела 7 настоящей Инструкции;
- новый вводимый пароль не должен повторять пять ранее введенных сотрудником паролей.

6.5 В случае компрометации или подозрения на компрометацию пароля сотрудник банка должен сообщить в соответствующее подразделение ДИТ или Сектор автоматизации, компьютеризации и внедрения ИКТ областных и районных филиалов, которые должны известить системного администратора для блокировки доступа по учетной записи и формирования нового инициализационного пароля.

6.6 Плановая смена паролей доступа к серверному, сетевому оборудованию и средствам защиты информации должна производиться ответственными за их эксплуатацию администраторами не реже одного раза в 3 месяца.

Выполнение требования периодической смены паролей со стороны администраторов контролируется УИБ ДИББ и Отделом по безопасности, режиму и защите информации областных филиалов.

6.7 В случае компрометации или подозрения на компрометацию пароля административных учетных записей, администратор обязан немедленно сменить его.

6.8 Плановая смена криптографических закрытых ключей ЭЦП должна производиться УИБ ДИББ через каждые 2 года, исходя из срока действия сертификата открытых ключей ЭЦП.

6.9 В случае компрометации или подозрения на компрометацию криптографического закрытого ключа ЭЦП сотрудник банка обязан немедленно сообщить в подразделение информационной безопасности, который должен известить администратора Центра регистрации ЭЦП для приостановления или отзыва сертификата открытого ключа ЭЦП и создание нового криптографического ключа и сертификата.

6.10 Внеплановая смена пароля и криптографических ключей, удаление учетной записи пользователя и сертификата открытых ключей в случае прекрашения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя в системе.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на

другую работу и другие обстоятельства) администратора информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной зашитой.

6.11 Доступ к объектам информатизации по учетной записи должен блокироваться после трех неудачных попыток ввода неверного пароля.

6.12 При неиспользовании криптографических ключей (завершение рабочего дня, выход в отпуск или на больничный и т.д.) сотрудник банка обязан сдать его начальнику своего подразделения или подразделение информационной безопасности. Неиспользуемые криптографические ключи должны храниться в сейфах.

7. Требования к формированию паролей

7.1 При формировании паролей доступа к объектам информатизации АО «Узнацбанк» должны выполняться следующие требования:

- минимальная длина пароля составляет не менее 8-ми символов;
- пароль должен состоять из комбинации цифр, букв латинского алфавита верхнего и нижнего регистра, а также символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.);
- при смене пароля новое её значение должно отличаться от предыдущего не менее чем в 6 позициях.

7.2 Указанные в пункте 7.1 требования должны распространяться на пароли доступа к закрытому ключу ЭЦП, используемому сотрудником АО «Узнацбанк» для работы в ИАБС.

7.3 Пароль администратора базы данных информационных систем должен быть не менее 12 символов с использованием букв нижнего и верхнего регистра, цифр и специальных символов.

8. Контроль над действиями пользователей и обслуживающего персонала при работе с паролями и криптографическими ключами

8.1 Контроль за действиями пользователей и обслуживающего персонала при работе с паролями и криптографическими ключами возлагается на подразделения информационной безопасности.

8.2 Контроль за действиями пользователей и обслуживающего персонала при работе с паролями производится подразделениями информационной безопасности не реже одного раза в 6 месяцев.

8.3 При контроле за действиями пользователей и обслуживающего персонала при работе с паролями и криптографическими ключами проверяется выполнение ими:

- требований по формированию паролей в соответствии с разделом 7 настоящей Инструкции;
- требований по хранению паролей и криптографических ключей в соответствии с настоящей Инструкцией;

- обязанностей владельцев паролей, изложенных в разделе 9 настоящей Инструкции;

- обязанностей владельцев криптографических ключей, изложенных в Инструкции по организации криптографической защиты информации.

8.4 При контроле проверяется правильность настроек службы Active Directory Windows Server и систем управления доступом пользователей в информационных системах.

Выборочная проверка пользователей по обеспечению сохранности ими своих паролей (опрос, анкетирование, проверка).

Проверка обслуживающего персонала по сложности вводимого им пароля и способах его хранения.

8.5 В случая выявления нарушения требований настоящей Инструкции сотрудники подразделений информационной безопасности обязаны дать предупреждение сотруднику для недопущения повторного нарушения.

8.6 О случаях систематического или грубого нарушения требований настоящей Инструкции сообщается директору ДИББ для принятия им соответствующих мер в отношении нарушителя.

9. Обязанности и ответственность

9.1 Владельцы паролей обязаны:

- применять различные пароли для каждой учетной записи при доступе к разным объектам информатизации;
- информировать о компрометации своего пароля для блокировки доступа по учетной записи и старому паролю, а также для внеплановой смены пароля;
- обеспечивать сохранность пароля;
- не сообщать учетные записи и пароли другим сотрудникам банка и посторонним лицам.

9.2 Владелец пароля обязан применять адекватные меры по защите своих паролей, в том числе:

- запоминать свои пароли или хранить их таким образом, чтобы они были недоступны другим лицам;
- не передавать свои пароли никому, ни под каким предлогом, включая своих коллег, за исключением непосредственного руководителя структурного подразделения;
- при использовании пароля (например, его вводе) принять необходимые меры, исключающие возможность его компрометации (например, исключить возможность визуального просмотра вводимого пароля).

9.3 Запрещается применять пароли, используемые владельцем во внешних от АО «Узнацбанк» системах (например, на веб-сайтах сети Интернет, Интернет-магазинах, электронных платежных системах и др.).

9.4 Обязанности и ответственность владельцев криптографических ключей определены в Инструкции по организации криптографической защиты информации и должны выполняться сотрудниками банка.

9.5 Обязанности и ответственность клиентов банков по сохранности своих паролей и криптографических ключей должны оговариваться в заключаемых ими договорах на оказание банковских услуг.

9.6 Администраторам запрещено хранить пароли пользователей в открытом виде, а также размещать пароли на ресурсах общего доступа, или пересылать их по электронной почте, за исключением пересылки пользователю инициализационного пароля (исключительно только корпоративной электронной почтой).

9.7 Подразделения информационной безопасности обязаны:

- консультировать сотрудников по вопросам использования парольной защиты и криптографических ключей, обеспечения сохранности паролей и криптографических ключей и несение ответственности за их компрометацию;
- немедленно сообщать в УИБ ДИББ о любых случаях нарушений настоящей Инструкции со стороны сотрудников банка.

9.8 Владельцы паролей и криптографических ключей, сотрудники, формирующие и выдающие их, несут ответственность за их сохранность и выполнение требований настоящей Инструкции.

10. Ответственность

10.1 Сотрудники и администраторы, формирующие пароли, несут ответственность за выполнения требований настоящей Инструкции.

10.2 Сотрудники АО «Узнацбанк» несут ответственность за обеспечение сохранности своих паролей и иных идентификаторов доступа к объектам защиты согласно требованиям настоящей Инструкции.

Приложение №8
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-б 27.12.2021г

Инструкция по антивирусной защите

1. Общие положения

1.1 Настоящая Инструкция определяет порядок организации и требования обеспечения защиты информации и банковской информационной инфраструктуры АО «Узнацбанк» от действий вредоносных программ.

1.2 Настоящая Инструкция является обязательной для исполнения всеми сотрудниками АО «Узнацбанк» при пользовании банковской информационной инфраструктурой АО «Узнацбанк», а также сотрудниками, ответственными за обеспечение антивирусной защиты.

2. Термины и определения

2.1 В настоящей Инструкции применены следующие термины и их определения:

антивирусная защита - комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий компьютерного вируса при помощи антивирусных программ;

антивирусная программа - специализированное программное обеспечение, имеющее в своем составе механизм обнаружения, лечения и удаления вредоносных программ, включая вирусы, сетевые черви, трояны, фишинговые ссылки и т.д;

антивирусный контроль - проведение на постоянной основе проверки наличия вредоносных программ на рабочих станциях и серверах, ежедневное их обновление, ежемесячное полное сканирование рабочих станций и серверов на наличие вредоносного программного обеспечения, реагирование на инциденты, связанные с обнаружением вредоносных программ;

вредоносная программа: программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий;

средство антивирусного контроля - автоматизированная система централизованного контроля параметров, обновления антивирусного средства и произошедших инцидентов в области антивирусной защиты.

3. Общие требования

3.1 Для обеспечения информационной безопасности к использованию в АО «Узнацбанк» допускаются только лицензионные антивирусные средства.

3.2 Не допускается подключение к ЛВС АО «Узнацбанк» рабочих станций и серверов, на которых не установлены антивирусные средства.

3.3 В АО «Узнацбанк» применяются системы централизованного управления антивирусными программами, установленными на рабочих станциях и серверах (далее – централизованная антивирусная система):

- централизованная антивирусная система в г. Ташкенте, охватывающая все рабочие станции и сервера головного офиса и Главного управления по Ташкенту и его структурных подразделений в г. Ташкенте, включая минибанки;

- централизованная антивирусная система, установленная в каждом областном филиале и охватывающая все рабочие станции и сервера областного филиала и подчиненных ему районных филиалов и минибанков.

С развитием предусматривается применение одной единой централизованной антивирусной системы для АО «Узнацбанк».

3.4 Централизованная антивирусная система устанавливается на отдельном сервере, которая обеспечивает централизованный контроль функционирования и управление установленных на рабочих станциях и серверах антивирусов, а также централизованное обновление их антивирусных баз.

Управляемые централизованной антивирусной системой антивирусы устанавливаются на каждой рабочей станции и серверах, используемых в АО «Узнацбанк».

3.5 Сервера централизованной антивирусной системы должны размещаться в защищенных помещениях ЦОД и коммутационных помещениях областных филиалов.

3.6 Обязательному антивирусному контролю подлежат все рабочие станции, сервера и сетевой трафик.

3.7 Об обнаружении компьютерного вируса в АО «Узнацбанк» УИБ ДИББ информирует Центральный банк с указанием происхождения вируса и его типа.

4. Организация работ по антивирусной защите

4.1 Обслуживание и управление централизованной антивирусной системой в г. Ташкенте осуществляется ответственным сотрудником УИБ ДИББ, а централизованными антивирусными системами в областных филиалах – ответственным сотрудником Отделов по безопасности, режиму и защите информации областных филиалов (администраторы информационной безопасности областных филиалов).

4.2 Установка и настройка средств антивирусного контроля на рабочих станциях и серверах осуществляется сотрудниками УИБ ДИББ, Отделов по безопасности, режиму и защите информации областных филиалов и главным специалистом по безопасности, режиму и защите информации районных филиалов (далее – подразделения информационной безопасности).

4.3 В настройках межсетевых экранов и средств IDPS должен быть включен контроль трафика на наличие вредоносных программ.

4.4 Антивирусный контроль всех загрузочных секторов дисков и файлов рабочих станций должен проводиться ежедневно в автоматическом режиме при начальной загрузке рабочих станций, а серверов - при их перезапуске.

4.5 Обновление баз антивирусных средств, установленных на рабочих станциях и серверах, должно проводиться регулярно в автоматическом режиме с централизованной антивирусной системы. Централизованная антивирусная система должна быть настроена на доступ к серверам обновлений разработчика антивирусного средства.

4.6 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по ЛВС АО «Узнацбанк» и корпоративной сети, а также на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

4.7 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в год.

4.8 Установка (изменение) системного и прикладного программного обеспечения должна осуществляться сотрудниками подразделений информационной безопасности. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вредоносной программы. Непосредственно после установки (изменения) системного программного обеспечения, должна проводиться антивирусная проверка.

4.9 Для исключения самостоятельной установки сотрудниками банка программного обеспечение на рабочих станциях, им должен предоставлять пользовательский (не администраторский) доступ к своим рабочим станциям.

4.10 Настройки антивирусных средств, установленных на рабочих станциях и серверах, производится сотрудниками подразделений информационной безопасности в соответствии с требованиями, устанавливаемыми УИБ ДИББ.

Возможности сотрудников по изменению настроек антивирусных средств, его остановке или удалению, должны быть ограничены.

5. Требования к участникам работ по антивирусной защите

5.1 Запрещается эксплуатация рабочих станций и серверов без установленного антивирусного программного обеспечения.

Антивирусное программное обеспечение должно поддерживаться в актуальном состоянии.

5.2 При возникновении подозрения на наличие вредоносного программного обеспечения (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках) сотрудник банка самостоятельно или вместе с сотрудником подразделения информационной

безопасности должен провести антивирусный контроль своей рабочей станции.

5.3 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники банка обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов сотрудника подразделения информационной безопасности, а также сотрудников, использующих эти файлы в работе;
- провести анализ дальнейшего его использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, сообщить об этом сотруднику подразделения информационной безопасности.

5.4 В случае заражения рабочей станции или сервера компьютерным вирусом, для исключения его распространения по сети АО «Узнацбанк» должны приниматься следующие оперативные меры:

- приостановить работу на зараженной рабочей станции или сервере и отключить его от сети, выдернув сетевой кабель;
- произвести поиск и удаление вируса с применением лицензионного антивирусного средства;
- в случае невозможности удаления вируса антивирусным средством должна быть произведена переустановка операционной системы и программ на рабочей станции или сервере.

5.5 Пользователю рабочей станции запрещается без одобрения подразделения информационной безопасности:

- изменять настройки и конфигурацию средств антивирусной защиты;
- удалять или добавлять в систему какие-либо другие средства антивирусной защиты;
- использовать на рабочей станции съемные носители информации без предварительной проверки установленными средствами антивирусной защиты;
- запускать неизвестные приложения, пришедшие по электронной почте.

5.6 Сотрудник банка обязан:

- не открывать вложения к сообщениям электронной почты, полученным из неизвестных, подозрительных или не доверенных источников. Такие вложения должны незамедлительно удаляться;
- не скачивать информацию из неизвестных или подозрительных источников;
- избегать предоставление общего доступа к логическим дискам с правами чтения/записи, в случае если это не требуется в рамках выполнения основной деятельности;
- перед использованием носителя информации, полученного от неизвестных или подозрительных источников, сканируйте его на отсутствие вирусов;

- ежедневно при начальной загрузке рабочей станции убедиться в наличии резидентного антивирусного монитора и в случае его отсутствия уведомить об этом подразделение информационной безопасности;

- самостоятельно запускать внеплановую антивирусную проверку рабочей станции при получении от подразделения информационной безопасности уведомления о наличии в системе вируса, а также при возникновении подозрения на наличие вируса.

6. Ответственность участников работ по антивирусной защите

6.1 Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на подразделения информационной безопасности.

6.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на начальника УИБ ДИББ и начальников Отделов по безопасности, режиму и защите информации областных филиалов.

6.3 Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками АО «Узнацбанк» осуществляется УИБ ДИББ, Отделами по безопасности, режиму и защите информации областных филиалов и главными специалистами по безопасности, режиму и защите информации районных филиалов.

Приложение №9
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-б 27.12.2021г

Инструкция по обеспечению информационной безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных

1. Общие положения

1.1 Настоящая Инструкция определяет и устанавливает порядок использования и требования по обеспечению информационной безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных, используемых в АО «Узнацбанк».

1.2 Под использованием мобильных устройств и носителей информации в банковской информационной инфраструктуре АО «Узнацбанк» понимается их подключение к рабочей станции, серверу, ЛВС и/или корпоративной сети с целью обработки, приема/передачи информации между банковской информационной инфраструктурой и мобильными устройствами, а также носителями информации.

2. Термины и определения

2.1 В настоящей Инструкции применены следующие термины и их определения:

вредоносная программа: программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий;

контролируемая зона: пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

Примечание: Граница контролируемой зоны могут быть:

- периметр контролируемой территории организации;
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;

мобильные устройства - устройства вида смартфоны, Интернет планшеты, электронные книги, телефоны, карманные персональные компьютеры, ноутбуки, имеющие операционную систему и мобильные приложение, которые позволяют подключаться к сетям мобильной связи, Wi-Fi и Интернет, а также к рабочим станциям и другим аналогичным устройствам;

накопитель данных – устройство, осуществляющее чтение и/или запись информации, которые используются для резервного копирования и хранения информации, а также для её транспортировки;

съемный носитель информации - носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования. Они могут быт в виде: съемные жесткие диски, флэш-память, оптические лазерные диски (CD, DVD), дискеты.

3. Правила и требования применения мобильных устроиств

3.1 Запрещается применение мобильных устройств, принадлежащих сотрудникам АО «Узнацбанк»:

- в помещениях, где проводятся конфиденциальные переговоры и мероприятия конфиденциального характера;
- для подключения к ЛВС АО «Узнацбанк» и корпоративной сети, а также информационным системам;
- для подключения мобильных устройств удаленных пользователей к информационной системе и корпоративной сети через сеть телекоммуникаций общего пользования и Интернет;
- в качестве носителей конфиденциальной или иной защищаемой информации, включая пароли и криптографические ключи.

3.2 В головном офисе, областных и районных филиалах АО «Узнацбанк» могут применяться меры по запрещению использования в контролируемой зоне мобильных устройств сторонними лицами, имеющими разовый допуск, за исключением клиентов в помещениях 1-зоны (информационные и операционные залы, кредитные отделы).

3.3 В банковской информационной инфраструктуре АО «Узнацбанк» допускается использование только учтенных мобильных устройств, которые являются собственностью АО «Узнацбанк».

3.4 К учетным мобильным устройствам предъявляются те же требования по защите информации, что и для стационарных рабочих станций, и должны подвергаться периодической проверке на наличие вредоносных программ антивирусными средствами не реже одного раза в неделю.

3.5 Запрещается использовать учетные мобильные устройства для хранения любой конфиденциальной информации АО «Узнацбанк».

3.6 Учетные мобильные устройства допускается использовать для подключения к информационным система АО «Узнацбанк» только в пределах контролируемой зоны. При этом требования к ним предъявляются такие же, как и рабочим станциям в части аутентификации и криптографической защиты информации.

3.7 При использовании учетных мобильных устройств сотрудниками АО «Узнацбанк» должны выполняться следующие требования:

- использовать их по назначению и исключительно для выполнения своих служебных обязанностей;
- ставить в известность УИБ ДИББ в головном офисе, а в филиалах-Отделы по безопасности, режиму и защите информации областных филиалов и главного специалиста по безопасности, режиму и защите информации районных филиалов (далее – подразделения информационной безопасности) о любых фактах нарушения требований настоящей Инструкции;

- извещать подразделения информационной безопасности о фактах утраты (кражи) мобильных устройств;

- обеспечивать физическую безопасность мобильных устройств всеми разумными способами;

- не передавать мобильные устройства другим лицам.

3.8 При использовании учетных мобильных устройств сотрудникам АО «Узнацбанк» запрещено оставлять их без присмотра, если не предприняты меры по обеспечению их физической безопасности.

3.9 Для обеспечения информационной и физической безопасности мобильных устройств при их использовании за пределами АО «Узнацбанк» (командировки, встречи, переговоры и т.п.) должны применяться следующие меры:

- установка пароля доступа или использование средств аутентификации на основе биометрических данных пользователя при доступе к мобильному устройству;

- установка пароля доступа к определенным приложениям мобильного устройства;

- установка и использование на мобильном устройстве средств антивирусной защиты и персонального firewall;

- использование при необходимости шифрование данных на мобильном устройстве для защиты хранящихся персональных данных.

4. Правила и требования применения съемных носителей и накопителей данных

4.1 В банковской информационной инфраструктуре АО «Узнацбанк» допускается использование только учтенных накопителей данных и съемных носителей информации, которые являются собственностью АО «Узнацбанк» и подвергаются регулярной ревизии и контролю со стороны подразделений информационной безопасности.

4.2 Учетные накопители данных и съемные носители информации должны подвергаться периодической проверке на наличие вредоносных программ антивирусными средствами не реже одного раза в неделю.

4.3 Вынос за пределы контролируемой зоны учетных накопителей данных и съемных носителей информации производится только с разрешения директора ДИББ.

В разрешении на вынос учетных накопителей данных и съемных носителей информации указываются:

- Ф.И.О. и должность сотрудника, пользующимся устройством;

- модель и учетный номер устройства;

- причина выноса (командировки, встречи, переговоры и т.п.);

- период действия разрешения.

Не допускается вынос за пределы контролируемой зоны накопителей данных и съемных носителей, используемых для хранения конфиденциальной информации.

4.4 Накопители данных и съемные носители, используемые для хранения конфиденциальной информации, подлежат учету подразделениями информационной безопасности в журнале, форма которой определена в приложении к настоящей Инструкции.

Накопители данных и съемные носители, содержащие конфиденциальные данные, должны быть промаркированы нанесением зеленой, желтой или оранжевой наклейки (стикера) с надписью «NBU».

Все промаркированные съемные носители информации и накопители, предназначенные для хранения и передачи конфиденциальной информации, должны быть инвентаризованы в подразделениях информационной безопасности. Проверка носителей и наличия маркировки на них, производится подразделениями информационной безопасности не реже раза в год.

4.5 При использовании накопителей данных и съемных носителей информации сотрудниками банка должны выполняться следующие требования:

- использовать их по назначению и исключительно для выполнения своих служебных обязанностей;
- ставить в известность подразделения информационной безопасности о любых фактах нарушения требований настоящей Инструкции;
- извещать подразделения информационной безопасности о фактах утраты (кражи) или выхода из строя накопителей данных и съемных носителей информации;
- обеспечивать физическую безопасность накопителей данных и съёмных носителей информации всеми разумными способами;
- не передавать носители информации другим лицам.

4.6 При использовании учетных накопителей данных и съемных носителей информации сотрудникам банка запрещено оставлять их без присмотра, если не предприняты меры по обеспечению их физической безопасности.

4.7 В случае необходимости проведения ремонта рабочей станции или сервера сторонними организациями перед началом проведения ремонта должен быть извлечен накопитель данных (HDD). В случаях, когда проведение ремонта невозможно без накопителя данных, указанные ремонтные работы должно контролироваться со стороны сотрудника банка.

4.8 Требования к учету, использованию, хранению и уничтожению защищенных съемных носителей, используемых для хранения криптографических ключей, определены в Инструкции по организации криптографической защиты информации, приведенной в приложении №15 к Политике информационной безопасности АО «Узнацбанк».

5. Порядок передачи, списания и уничтожения

5.1 В случае увольнения или перевода сотрудника банка на другое место работы, предоставленные ему мобильные устройства, накопители данных и съемные носители информации, принадлежащие АО «Узнацбанк»,

сдаются в Отдел технической методологии и учета техники ДИТ, а в филиалах – в Сектор автоматизации, компьютеризации и внедрения ИКТ.

5.2 Вышедшие из строя или предназначенные к уничтожению носители, устройства и накопители, в том числе те, на которых находились конфиденциальные данные, должны храниться в запираемых металлических шкафах (сейфах).

5.3 После принятия решения о снятии с эксплуатации мобильных устройств, съемных носителей и накопителей данных должна быть произведена процедура их уничтожения (утилизации) с составлением акта уничтожения.

5.4 При утилизации непригодных к дальнейшей эксплуатации мобильных устройств, съемных носителей и накопителей данных, они должны подвергаться очистке информации путем удаления информации и форматирования носителей информации и физическому уничтожению. Физическое уничтожение устройств не должно позволять считывать с неё остаточную информацию, для чего должны быть уничтожены все микросхемы с помощью молотка.

5.5 При передаче мобильных устройств, съемных носителей и накопителей данных, не содержащих конфиденциальную информацию, другому сотруднику, хранящаяся в этих устройствах информация должна быть уничтожена методами удаления всех данных, а для носителей и накопителей данных – путем их форматирования.

5.6 В случае необходимости удаления конфиденциальной информации со съемных носителей информации и накопителей данных должны использоваться средства гарантированного уничтожения информации или прибегаться к услугам специализирующих организаций, имеющих данные средства.

6. Ответственность

6.1 Сотрудники банка несут персональную ответственность за нарушение настоящей Инструкции.

6.2 Нарушение правил пользования съемных носителей данных, мобильных устройств, накопителей данных, установленных настоящей Инструкцией, влечёт за собой наложение дисциплинарной ответственности в соответствии с внутренним трудовым распорядком и трудовым законодательством Республики Узбекистан.

6.3 Подразделения информационной безопасности ответственны за обеспечение контроля выполнения настоящей Инструкции сотрудниками банка.

Приложение
к Инструкции по обеспечению
информационной безопасности при
работе со съемными носителями
данных, мобильными устройствами,
накопителями данных

ЖУРНАЛ
учета накопителя данных и съемных носителей информации

Дата, учетный номер	Тип накопителя данных и съемных носителей информации (жесткий диск, ГМД, CD, DVD диски, USB- носители, и т.д.), объем памяти, наименование и заводской номер	Расписка о получении (Ф.И.О., подпись получателя, дата)	Расписка об обратном приеме (Ф.И.О. и подпись принимателя, дата)	Место хранения съемных носителей информации (номер сейфа, шкафа, стеллажа)	Отметка об уничтожении съемных носителей информации (подпись администратора, дата)	Примечание
1	**2**	**3**	**4**	**5**	**6**	**7**

Приложение №10
к Политике информационной
безопасности АО «Узнацбанк»
№124-б 27.12.2021г.

Правила по разработке матрицы доступа к информационным ресурсам

1. Общие положения

1.1 Настоящие Правила описывают процедуру разработки матрицы доступа к информационным ресурсам АО «Узнацбанк».

Требования настоящих Правил является обязательным для информационных ресурсов, принадлежащих АО «Узнацбанк».

1.2 Правила (политика) разграничения доступа к информационным ресурсам формируются матрицей доступа, в которой указывается, каким субъектам (группам субъектов), к каким объектам (группам объектов), какие права доступа (чтение, запись, исполнение и т.д.) разрешены либо запрещены.

1.3 ДИТ совместно с ДИББ по согласованию с руководителями заинтересованных подразделений разрабатывает матрицу доступа к информационным ресурсам АО «Узнацбанк».

1.4 Матрицей доступа определяется категория пользователей, получающих доступ к информационным ресурсам АО «Узнацбанк», а также их права и полномочия по доступу и обработке информации.

На основе матрицы доступа осуществляется управление доступом пользователей к информационным ресурсам.

Категории пользователей – это объединенная группа сотрудников АО «Узнацбанк» по признакам функциональных обязанностей, роду деятельности, выполняемой работы, должности и др.

1.5 Матрица доступа разрабатывается ДИТ и реализуется системными администраторами информационных систем путем внедрения и применения в информационных ресурсах средств аутентификации и авторизации пользователей на основе предъявляемых ими идентификаторов.

2. Термины и определения

2.1 В настоящих Правилах применены следующие термины и их определения:

матрица доступа - таблица, отображающая права разграничения доступа;

право на доступ - разрешение субъекту на получение доступа к объекту в рамках своих полномочий.

3. Требования по разработке матрицы доступа

3.1 Матрица доступа к информационным ресурсам (базам данных) информационных систем определяются в технических заданиях и требованиях на их создание или модернизацию информационных систем и реализуются при разработке прикладной программы информационных систем.

3.2 Матрица доступа к информационным ресурсам (файлы, папки, устройства, службы и отдельные базы данных), не входящих в состав информационных систем разрабатываются ДИТ исходя из уровня допуска персонала к информации указанных информационных ресурсов.

ДИТ должен вестись список указанных информационных ресурсов, для которых требуется определение матрицы доступа.

3.3 Разработка матрицы доступа к информационным ресурсам осуществляется в следующем порядке:

1) формируется список информационных ресурсов (файлы, папки, устройства, службы, базы данных);

2) для каждого информационного ресурса формируется список пользователей, которые будут иметь право доступа к нему;

3) список пользователей разбивается на категории пользователей с указанием их прав и полномочий доступа, при этом учитывается занимаемая должность, функциональные обязанности и полномочия сотрудников;

4) внедрение процедур получения разрешения.

3.4 Матрица доступа для каждого информационного ресурса в отдельности и должна включать в себя:

1) список пользователей, которые будут иметь право доступа к нему;

2) перечень категорий пользователей с указанием их прав и полномочий доступа,

3) процедуры получения разрешения.

При определении категорий пользователей учитывается занимаемая должность, функциональные обязанности и полномочия сотрудников.

В случае необходимости для отдельных информационных ресурсов в матрице доступа могут указываться расписание доступа к информационному ресурсу для категории или конкретного пользователя в соответствии с закрепленными за ними правами, т.е. в какой период времени можно получать доступ к информационному ресурсу.

3.5 Пользователям информационных ресурсов могут предоставляться следующие права и полномочия:

- Read (R) - получение информации из объекта;
- Write (W) - обновление информации в объекте;
- Append (A) - добавление в объект новой информации;
- Execute (E) - интерпретация объекта как исполняемого кода;
- Delete (D) - уничтожение объекта;
- GetInfo (G) - получение информации об объекте;
- SetInfo (S) - установка информации об объекте;
- Privilege (P) - установка прав доступа к объекту.

3.6 При разработке матрицы доступа должны учитываться следующие требования:

- различия между обязательными и рекомендуемыми для использования правилами, которые применяются при определенных условиях;

- формулировать правила, основываясь на предпосылке «все должно быть в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;

- изменения уровня конфиденциальности информации, генерируемых автоматически средствами обработки информации и инициируемых по усмотрению пользователей;

- изменения прав пользователя, устанавливаемых автоматически информационной системой и определенных администратором;

- правила, требующие и не требующие специального согласования перед введением в действие.

3.7 Разработанная матрица доступа согласовывается с ДИББ и заинтересованными подразделениями АО «Узнацбанк» и утверждается директором ДИТ.

3.8 На основе матрицы доступа реализуются системы разграничения доступа к информационным ресурсам по правам и ролям, предоставленным сотрудникам АО «Узнацбанк».

3.9 Для получения разрешения на использование новых средств обработки информации при доступе к информационным ресурсам должны выполняться следующие мероприятия:

- новые средства и их назначение должны быть утверждены руководством и согласованы с директором ДИТ;

- необходимо проводить тестирование программно-аппаратных средств на совместимость с другими компонентами системы до момента внедрения;

- использование личных технических средств информатизации (например, ноутбуков, домашних компьютеров и т.д.) на рабочем месте для обработки служебной информации должно быть запрещено.

3.10 Матрица доступа к основным информационным ресурсам АО «Узнацбанк» приведена в приложении к настоящим Правилам.

Приложение
к Правилам по разработке матрицы
доступа к информационным ресурсам
АО «Узнацбанк»

Матрица доступа к основным информационным ресурсам АО «Узнацбанк»

Пользователи	ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Головной офис							
Руководство							
Председатель Правления	R	R	R	R,W			
Первый заместитель Председателя	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Заместитель Директора Департамента	R	R	R	R,W			
Советник Председателя Правления Банка по правовым-юридическим вопросам	R	R	R	R,W			
Советник Председателя Правления по вопросам повышения эффективности духовно-просветительской работы и соблюдения законодательства о государственном языке	-	-	R	R,W			
Управляющий директор по кредитованию	R	R	R	R,W			
Управляющий Директор розничного блока	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Исполнительный аппарат Узнацбанка								
Начальник Исполнительного Аппарата		R	R		R,W			
Заместитель Начальника Исполнительного Аппарата		R	R	A	R,W			
Делопроизводитель		-	-	R	R,W			
Секретариат	Первый помощник Председателя Правления-Заместитель Начальника Исполнительного Аппарата	R	R	R	R,W			
	Помощник Председателя Правления	-	R	R	R,W			
	Помощник Заместителя Председателя Правления	-	R	R	R,W			
	Помощник Заместителя Председателя Правления	R	R	R	R,W			
	Помощник Заместителя Председателя Правления	R	R	R	R,W			
	Помощник Заместителя Председателя Правления	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Управление координации исполнения поручений, данных в ходе визитов Президента Республики Узбекистан в регионы	Начальник Управления	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел координации исполнения поручений, данных в ходе визитов	Заместитель Начальника Управления-Начальник отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел координации программ регионального развития и свободных экономических, малых промышленных зон	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Управление контроля исполнительской дисциплины и работ с обращениями	Начальник Управления	R	R	R	R,W			
Отдел контроля исполнительной дисциплины и работы с обращениями	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	A	R,W			
	Главный специалист	R	R	A	R,W			
	Главный специалист	R	R	A	R,W			
	Ведущий специалист	R	R		R,W			
Канцелярия	Начальник Отдела	-	R	A	R,W			
	Главный специалист	-	R	A	R,W			
	Ведущий специалист	-	R	A	R,W			
	Ведущий специалист	-	R	A	R,W			
	Ведущий специалист	-	R	A	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист	-	R	A	R,W			
	Специалист 1-категории	-	R	A	R,W			
Департамент юридической службы								
Директор Департамента		-	R	R	R,W			
Помощник юрисконсульта		-	R	R	R,W			
Практика договорной и корпоративной работы	Заместитель Директора Департамента-Руководитель практики	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
Практика правовой защиты интересов банка в судах и иных органах	Заместитель Директора Департамента-Руководитель практики	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Юрисконсульт	-	R	R	R,W			
	Помощник юрисконсульта	-	R	R	R,W			
Отдел методологии	Начальник Отдела	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Департамент внутреннего контроля								
Директор Департамента		R	R	-	R,W			
Делороизводитель		-	R	-	R,W			
Отдел мониторинга грантов	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел проверок нарушений и мониторинга возмещения вреда, нанесенного Банку	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Управление внутреннего контроля по ПЛПД/ФТ/ФРОМУ	Начальник Управления	R	R	R	R,W			
Отдел внутреннего контроля банковских операций в национальной валюте в сфере ПЛПД/ФТ/ФРОМУ	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел внутреннего контроля банковских операций в иностранной валюте в сфере ПЛПД/ФТ/ФРОМУ	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел мониторинга соблюдения законодательства в сфере ПЛПД/ФТ/ФРОМУ	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел внутреннего контроля операций МБРЦ в сфере ПЛПД/ФТ/ФРОМУ	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление ревизии деятельности кассы и валютно-обменных пунктов	Начальник Управления	R	R	R	R,W			
Отдел ревизии кассовых операций	Начальник отдела-Заместитель Начальника Управления	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел ревизии деятельности валютно-обменных пунктов	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Управление координации и мониторинга аудиторских проверок	Заместитель Директора Департамента-Начальник Управления	R	R	R	R,W			
Отдел внедрения международного банковского аудита и методологии	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел мониторинга результатов аудиторских проверок	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление аудиторской службы	Начальник Управления	R	R	R	R,W			
Отдел аудита корпоративного бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел аудита розничного бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел аудита подразделений поддержки бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Департамент внутреннего аудита								
Директор Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R	R	R	R,W			
Делопроизводитель		R	R	R	R,W			
Управление координации и мониторинга аудиторских проверок	Заместитель Директора Департамента-Начальник Управления	R	R	R	R,W			
Отдел внедрения международного банковского аудита и методологии	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел мониторинга результатов аудиторских проверок	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление аудиторской службы	Начальник Управления	R	R	R	R,W			
Отдел аудита корпоративного бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел аудита розничного бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел аудита подразделений поддержки бизнеса	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Первый отдел		R	R	R	R,W			
	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Второй отдел		R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Департамент по работе с персоналом								
Директор Департамента		-	R	R	R,W			
Заместитель Директора Департамента по делам молодежи		-	R	R	R,W			
Заместитель Директора Департамента		-	R	R	R,W			
Управление по работе с отделениями и филиалами	Начальник управления – Заместитель Директора Департамента	-	R	R	R,W			
	Начальник Отдел	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел по работе с кадрами отделений и филиалов	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Отдел подбора кадров по отделениям/филиалам и работе с резервом кадров	Начальник Отдела	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Специалист 1-категории	-	R	R	R,W			
Отдел отчетности и анализа	Начальник Отдела	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Сектор по отбору кадров и их адаптации	Заведующий сектором	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Управление по обучению и развитию персонала	Начальник управления	-	R	R	R,W			
Отдел по развитию корпоративной культуры, карьерного роста и мотивации персонала	Начальник Отдела	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Пресс-служба								
	Пресс-секретарь-Советник Председателя Правления	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Департамент информационной и банковской безопасности								

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Директор Департамента		W	R	R	R,W			
Отдел координации безопасности отделений и филиалов	Начальник Отдела	A	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Управление информационной безопасности		R	R	R	R,W			
Отдел безопасности информационных технологий	Начальник Отдела	R	R	R	R,W	R		Администратор
	Главный специалист	R	R	R	R,W			R
	Главный специалист	R	R	R	R,W			R
	Главный специалист	R	R	R	R,W			R
	Главный специалист	R	R	R	R,W			R
Отдел анализа и управления информационными рисками	Начальник Отдела	R	R	R	R,W			Администратор
	Главный специалист	R	R	R	R,W			R
	Главный специалист	R	R	R	R,W			R
Отдел технических средств защиты	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Управление охраны	Начальник управления	-	R	R	R,W			
	Начальник Отдела	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел охраны Головного банка и мониторинга охраны филиалов и отделений	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
	Начальник Отдела	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел безопасности Галереи изобразительного искусства Узбекистана	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
	Инспектор по охране и режиму	-	R	R	R,W			
Управление комплаенс контроля и противодействия коррупции	Начальник Управления	R	R	R	R,W			
Отдел комплаенс контроля и противодействия коррупции в филиалах	Начальник отдела-Заместитель Начальника Управления	R	R	R	R,W			
	Главный специалист	R	R	R				
	Главный специалист	R	R	R				
	Главный специалист	R	R	R				
Информационно-аналитический отдел	Начальник Отдела	R	R	R				
	Главный специалист	R	R	R				
	Главный специалист	R	R	R				

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист	R	R	R				
Департамент бухгалтерского учета и отчетности								
Директор Департамента - главный бухгалтер		A	R	R	R,W			
Заместитель главного бухгалтера по внедрению стандартов МСФО		W	R	R	R,W			
Управление формирования политики бухгалтерского учета и учетных процессов	Заместитель Главного бухгалтера-Начальник управления	A	R	R	R,W			
Отдел политики бухгалтерского учета и методологии	Главный специалист	W	R	R	R,W			
Отдел организации и контроля учетных процессов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел контроля учетных процессов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Управление финансовой отчетности	Начальник управления	R	R	R	R,W			
Отдел бухгалтерской и сводной отчетности	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел формирования консолидированной финансовой отчетности по МСФО	Заместитель Начальника Управления-Начальник отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Служба итогового контроля	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Служба финансового контроля	Заместитель Главного бухгалтера-Начальник службы	W	R	R	R,W			
Отдел контроля операционных расходов	Заместитель начальника службы-Начальник отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел организации налогового учета и налогообложения	Заместитель начальника службы-Начальник отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел налоговой отчетности и мониторинга по налоговым расходам	Главный специалист	W	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Сектор по мониторингу деятельности хозяйствующих единиц, находящихся в ведении Банка	Заведующий сектором	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Департамент розничного бизнеса								
Директор Департамента		W	R	R	R,W			
Заместитель Директора Департамента		W	R	R	R,W			
Делопроизводитель		-	-	R	R,W			
Управление аналитики, отчета, вкладных операций, денежных переводов и розничного бизнеса	Начальник Управления	W	R	R	R,W			
Отдел аналитики, бухгалтерского учета и отчетности	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел вкладных операций и денежных переводов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел развития локальных платежных систем	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Управление технической поддержки платёжных систем	Начальник Управления	W	R	R	R,W		W/R	
Отдел организации процессинга платёжных систем	Начальник Отдела	W	R	R	R,W		R	
	Главный специалист	W	R	R	R,W		R	
	Главный специалист	W	R	R	R,W		R	
	Главный специалист	W	R	R	R,W		R	
Отдел технической поддержки и ремонта оборудования	Начальник Отдела	W	R	R	R,W		-	
	Главный специалист	W	R	R	R,W		-	
	Главный специалист	W	R	R	R,W		-	
	Главный специалист	W	R	R	R,W		-	
Отдел мониторинга рисков по платежным системам	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Управление розничного кредитования	Начальник Управления	W	R	R	R,W			
Отдел верификации розничных кредитов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел аналитики и продаж розничных кредитов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист	R	R	R	R,W			
Управление продажи розничных продуктов	Начальник Управления	W	R	R	R,W			
Отдел разработки и внедрения новых продуктов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел розничных продаж	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Управление денежного обращения, эмиссионно-кассовой работы, конверсионных и валютно-обменных операций	Заместитель Директора Департамента-Начальник Управления	W	R	R	R,W			
Отдел денежного обращения	Начальник отдела-Заместитель Начальника Управления	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Начальник Отдела	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел организации эмиссионно-кассовой работы	Главный специалист	W	R	R	R,W			
Отдел конверсионных и валютно-обменных операций	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Управление маркетинга и связи с общественностью					R,W			
	Начальник Управления	R	R	R	R,W			
Отдел планирования и продвижения	Начальник Отдела	R	R	R	R,W			
	Бизнес аналитик	R	R	R	R,W			
	Менеджер по продвижению	R	R	R	R,W			
	Контент менеджер	R	R	R	R,W			
	Бренд менеджер	R	R	R	R,W			
Call-center	Начальник центра	R	R	R	R,W			
	Руководитель группы по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Оператор по входящим звонкам	R	R	R	R,W			
	Руководитель группы по исходящим звонкам	R	R	R	R,W			
	Оператор по исходящим звонкам	R	R	R	R,W			
	Оператор по исходящим звонкам	R	R	R	R,W			
	Оператор по исходящим звонкам	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Департамент казначейство								
Директор Департамента		W	R	R	R,W			
Заместитель Директора Департамента		W	R	R	R,W			
Делопроизводитель		-	-	R	R,W			
Управление валютных операций	Начальник Управления	W	R	R	R,W			
Отдел мониторинга внешнеторговых контрактов и проведения операций с драгметаллами	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел сводной отчетности по валютным операциям	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел конвертации и проведения операций на УзРВБ	Начальник Отдела	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Управление активов и пассивов	Начальник Управления	W	R	R	R,W			
Отдел управления ликвидностью	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел формирования и анализа казначейской отчетности	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел ценовой политики, планирования и анализа бюджета, процентных доходов и расходов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Управление дилинговых операций, валютной позицией и торговлей ценными бумагами	Начальник Управления	W	R	R	R,W			
Отдел дилинговых операций	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Начальник Отдела	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел валютной позитиции и Мидл-офис	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел торговли ценными бумагами	Начальник Отдела	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Департамент информационных технологий								
Директор Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R	R	R	R,W			
Заместитель Директора Департамента		-	R	R	R,W			
Делопроизводитель		-	R	R	R,W			
Отдел системного программного обеспечения	Начальник отдела СПО	-	R	R	R,W	R		
	Главный инженер-системный администратор	-	R	R	R,W	R		
	Ведущий инженер-системный администратор	-	R	R	R,W			
	Ведущий инженер-системный администратор	-	R	R	R,W			
	Ведущий инженер-системный администратор	-	R	R	R,W			
	Инженер-системный администратор	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Инженер-системный администратор	-	R	R	R,W			
	Инженер-системный администратор	-	R	R	R,W			
	Инженер-системный администратор	-	R	R	R,W			
Отдел сопровождения сетевой инфраструктуры	Начальник отдела ССИ	-	R	R	R,W			
	Главный сетевой инженер	-	R	R	R,W			
	Ведущий сетевой инженер	-	R	R	R,W			
	Ведущий сетевой инженер	-	R	R	R,W			
	Сетевой инженер	-	R	R	R,W			
Отдел технической методологии и учета техники	Начальник отдела ТМиУТ	-	R	R	R,W			
	Главный инженер по контролю технических средств	-	R	R	R,W			
	Ведущий инженер по контролю технических средств	-	R	R	R,W			
	Ведущий инженер по контролю технических средств	-	R	R	R,W			
	Ведущий инженер по контролю технических средств	-	R	R	R,W			
	Инженер по контролю технических средств	-	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление инновационного развития и внедрения новых продуктов	Начальник Управления	R	R	R	R,W			
Отдел управления проектами и бизнес-анализа	Начальник отдела УПиБА	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Бизнес-аналитик	R	R	R	R,W			
	Бизнес-аналитик	R	R	R	R,W			
Отдел разработки программного обеспечения	Начальник отдела РПО	-	R	Администратор	R,W			
	Главный программист	-	R	P,E,D	R,W			
	Главный программист	-	R	P,E,D	R,W			
	Ведущий программист	-	R	P,E,D	R,W			
	Ведущий программист	-	R	P,E,D	R,W			
	Ведущий программист	-	R	P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий программист	-	R	A,P,E,D	R,W			
	Ведущий программист	-	R	A,P,E,D	R,W			
	Программист	-	R	A,P,E,D	R,W			
	Программист	-	R	A,P,E,D	R,W			
	Программист	-	R	A,P,E,D	R,W			
	Программист	-	R	A,P,E,D	R,W			
	Тестировщик	-	R	R	R,W			
	Тестировщик	-	R	R	R,W			
	Веб-дизайнер	-	R	E	R,W			
	Веб-дизайнер	-	R	E	R,W			
Отдел консолидации данных и отчетности	Начальник отдела КДиО	W	R	R	R,W			
	Главный программист	W	R	R	R,W			
	Главный программист	W	R	R	R,W			
	Ведущий программист	R	R	R	R,W			
	Аналитик базы данных	R	R	R	R,W			
	Аналитик базы данных	R	R	R	R,W			
	Аналитик базы данных	R	R	R	R,W			
	Аналитик базы данных	R	R	R	R,W			
Управление поддержки информационных систем	Начальник Управления	W	R	R	R,W			
Отдел технологической поддержки ИС	Начальник отдела ТПИС	W	R	R	R,W			
	Главный специалист по программному обеспечению	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Специалист 1 категории по программному обеспечению	W	R	R	R,W			
	Специалист 1 категории по программному обеспечению	W	R	R	R,W			
	Специалист 1 категории по программному обеспечению	W	R	R	R,W			
	Специалист 1 категории по программному обеспечению	W	R	R	R,W			
Отдел эксплуатации ИС	Начальник отдела ЭИС	W	R	R	R,W			
	Главный специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Ведущий специалист по программному обеспечению	W	R	R	R,W			
	Начальник отдела СДБО	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел сопровождения дистанционного банковского обслуживания	Главный специалист по информационным технологиям	R	R	R	R,W			
	Ведущий специалист по информационным технологиям	R	R	R	R,W			
	Ведущий специалист по информационным технологиям	R	R	R	R,W			
	Специалист по информационным технологиям	R	R	R	R,W			
	Специалист по информационным технологиям	R	R	R	R,W			
	Специалист по информационным технологиям	R	R	R	R,W			
	Специалист по информационным технологиям	R	R	R	R,W			
Департамент по управлению рисками								
Директор Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R	R	R	R,W			
Делопроизводитель		-	-	R				

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление банковскими рисками	Начальник Управления	R	R	R	R,W			
Отдел рыночных рисков	Начальник Отдела	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел по управлению активами и пассивами банка и управление ликвидностью	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел операционных рисков	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Управление кредитными рисками	Начальник Управления	R	R	R	R,W			
Отдел кредитных рисков	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел координации андеррайтинга и калибровки скоринговой модели	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Информационно-аналитическое управление	Начальник Управления	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел аналитики рисков	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел анализа состояния рисков	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел методологии рисков	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Управление андеррайтинга и кредитного администрирования	Начальник Управления	W	R	R	R,W			
Отдел андеррайтинга	Начальник Отдела	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
	Андеррайтер	W	R	R	R,W			
Отдел кредитного администрирования	Начальник Отдела	W	R	R	R,W			
	Кредитный администратор	W	R	R	R,W			
	Кредитный администратор	W	R	R	R,W			
	Кредитный администратор	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Центр проектного финансирования								
Директор Центра		R	R	R	R,W			
Первый Заместитель Директора Центра		R	R	R	R,W			
Заместитель Директора Центра		W	R	R	R,W			
Управление экспертизы инвестиционных проектов	Начальник Управления	W	R	R	R,W			
Отдел экспертизы инвестиционных проектов ТЭК и индустрии	Начальник отдела -менеджер проекта	W	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
Отдел экспертизы инвестиционных проектов транспорта, телекоммуникаций и электротехнической промышленности	Менеджер проекта	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел экспертизы инвестиционных проектов текстильной и легкой промышленности	Начальник отдела -менеджер проекта	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел экспертизы инвестиционных проектов по повышению энергоэффективности промышленных предприятий,	Начальник отдела -менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
агропромышленного комплекса и прочее	Ведущий специалист	R	R	R	R,W			
Управление финансирования инвестиционных проектов и формирования отчетности	Начальник Управления	W	R	R	R,W			
Отдел корпоративного финансирования инвестиционных проектов	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Сектор формирования отчетности	Заведующий сектором	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Управление внешнеэкономической деятельности	Начальник Управления	W	R	R	R,W			
Отдел по работе с МФИ и привлечению иностранных кредитных линий	Начальник Отдела	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел протокола и установления корреспондентских отношений с иностранными банками	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел структурирования финансирования	Начальник Отдела	W	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел по работе с инвесторами	Начальник Отдела	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Главный специалист	R	R	R	R,W			
Управление мониторинга инвестиционных проектов	Начальник Управления	R	R	R	R,W			
	Заместитель Начальника Управления	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Департамент по корпоративным связям и инвестиции								
Директор Департамента		W	R	R	R,W			
Заместитель Директора Департамента		W	R	R	R,W			
Делопроизводитель		-	-	R	R,W			
Управление клиентских отношений	Заместитель Директора Департамента-Начальник Управления	W	R	R	R,W			
Отдел по взаимоотношению с клиентами	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел по работе с VIP клиентами и координации продаж	Начальник Отдела	W	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление инвестиций	Заместитель Директора Департамента-Начальник Управления	W	R	R	R,W			
Отдел по реализации и мониторингу проектов	Начальник Отдела	W	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Ассистент менеджера проекта	R	R	R	R,W			
Отдел по управлению портфельными инвестициями	Начальник Отдела	W	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Ассистент менеджера проекта	R	R	R	R,W			
Департамент развития сети и сервиса банка								
Директор Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R	R	R	R,W			
Делопроизводитель		-	-	R				
Управление развития и координации деятельности сети Банка	Начальник Управления	R	R	R	R,W			
	Заместитель Начальника Управления	R	R	R	R,W			
Сектор экономического анализа и координации деятельности сети банка	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Сектор развития и продвижения сети банка	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление развития сервиса и защиты прав потребителей банковских услуг	Начальник Управления	R	R	R	R,W			
	Заместитель Начальника Управления	R	R	R	R,W			
Отдел защиты прав потребителей банковских услуг	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 2-категории	R	R	R	R,W			
Сектор улучшения сервиса и кадрового потенциала	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Департамент развития молодежного предпринимательства								
Директор Департамента		R	R	R	R,W			
Управление развития молодежного предпринимательства	Заместитель Директора Департамента-Начальник Управления	R	R	R	R,W			
Отдел финансирования бизнес идей молодых предпринимателей	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел мониторинга молодежного предпринимательства и отчетности	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Начальник Отдела	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел обучения молодежи к предпринимательской деятельности, разработки инновационных проектов и методологии	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Call центр поддержки молодежного предпринимательства	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Департамент кредитования агросектора и контроля социальных программ								
Директор Департамента		R	R	R	R,W			
Делопроизводитель		-	-	R				
Управление кредитования и мониторинга проектов агросектора	Начальник Управления	W	R	R	R,W			
	Заместитель Начальника Управления	R	R	R	R,W			
Отдел кредитования хлопково-текстильных кластеров	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел кредитования проектов садоводства и овощеводства	Начальник Отдела	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел мониторинга и отчетности по программам широкого привлечения	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
населения к предпринимательству	Ведущий специалист	R	R	R	R,W			
Отдел мониторинга проектов агропромышленного сектора	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Кредитный департамент								
Директор Департамента		R	R	R	R,W			
Первый Заместитель Директора Департамента		W	R	R	R,W			
Управление кредитным портфелем, отчетности и одобрения кредитов	Первый заместитель директора департамента - Начальник управления	R	R	R	R,W			
	Заместитель Начальника Управления	R	R	R	R,W			
Отдел анализа, планирования кредитного портфеля и отчетности	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Отдел одобрения коммерческих кредитов	Начальник Отдела	R	R	R	R,W			
	Менеджер проекта	W	R	R	R,W			
Управление финансирования проектов	Начальник Управления	W	R	R	R,W			
	Заместитель Начальника Управления	W	R	R	R,W			
Отдел экспертизы инвестиционных проектов малого бизнеса	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ассистент менеджера	W		R	R,W			
Отдел выдачи гарантий и финансирования оборотного капитала	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Управление кредитования МСБ и торгового финансирования	Начальник Управления	W	R	R	R,W			
Отдел кредитования МСБ и торгового финансирования	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел контроля взаимодействия отделений с НИКИ и АСОКИ	Начальник Отдела	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Управление текущего мониторинга	Заместитель Директора Департамента-Начальник Управления	W	R	R	R,W			
	Заместитель Начальника Управления	W	R	R	R,W			
Отдел мониторинга инвестиционных проектов малого бизнеса	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел мониторинга гарантий и кредитов на оборотный капитал	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Департамент по работе с проблемными кредитами								
Директор Департамента		R	R	R	R,W			
Управление по взысканию и анализу проблемных кредитов отделений банка	Начальник Управления	W	R	R	R,W			
	Заместитель Начальника Управления	W	R	R	R,W			
Отдел по взысканию проблемных кредитов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
	Начальник Отдела	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Отдел анализа и отчетности проблемных кредитов	Главный специалист	W	R	R	R,W			
Управление по работе с кредитами в судебном разбирательстве отделений банка	Начальник Управления	W	R	R	R,W			
	Заместитель Начальника Управления	W	R	R	R,W			
Отдел правового сопровождения проблемных кредитов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел мониторинга и актуализации информации о проблемных кредитах	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Управление текущего мониторинга и сопровождения проектов	Начальник Управления	W	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
Департамент финансирования строительства и развития сферы услуг								
Директор Департамента		R	R	R	R,W			
Заместитель Директора Департамента		R,W	R	R	R,W			
Делопроизводитель		-	R	R	R,W			
Управление мониторинга и учета ресурсов	Начальник Управления	R,W	R	R	R,W			
			R	R	R,W			
	Начальник Отдела	R,W	R	R	R,W			

Пользователи		ИАБС	БИС
Отдел мониторинга кредитов, выданных физическим лицам	Главный специалист	W	R
	Ведущий специалист	W	R
Отдел мониторинга кредитов, выданных юридическим лицам	Начальник Отдела	R	R
	Менеджер проекта	R	R
	Менеджер проекта	R	R
Сектор учета привлеченных ресурсов и отчетности	Главный специалист	R	R
	Главный специалист	R	R
Управление кредитования	Начальник Управления	R,W	R
Отдел кредитования физических лиц	Начальник Отдела	W	R
	Главный специалист	W	R
	Главный специалист	W	R
Отдел кредитования юридических лиц	Начальник Отдела	R,W	R
	Менеджер проекта	R,W	R
	Ассистент менеджера	R,W	R
Управление капитального строительства	Начальник Управления	R,W	R
Отдел контроля хода строительства объектов	Начальник Отдела	R	R
	Главный специалист	R	R
Отдел подготовки проектной документации, договоров и конкурсных торгов	Заместитель Начальника Управления-Начальник отдела	R	R
	Главный специалист	R	R
	Ведущий специалист	R	R

	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			
	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Центр развития сферы услуг	Заместитель директора департамента-Начальник Центра развития сферы услуг	R	R	R	R,W			
Отдел сбора информации, изучения и анализ регионов	Заместитель начальника центра-Начальник отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Отдел разработки проектов, методологии, обучения и стандартизации продуктов сферы услуг	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Департамент стратегического развития банка								
Директор Департамента		R	R	R	R,W			
Первый Заместитель Директора Департамента		R	R	R	R,W			
Эксперт по разработке стратегии		R	R	R	R,W			
Делопроизводитель		-	-	R	R,W			
Управление стратегического планирования и мониторинга реализации	Начальник Управления	R	R	R	R,W			
Отдел стратегического планирования и экономического анализа банка	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
	Ведущий специалист	R	R	R	R,W			
Отдел мониторинга реализации стратегии	Начальник Отдела	R	R	R	R,W			
	Главный специалист	R	R	R	R,W			
Служба организации закупок	Начальник службы	R	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Менеджер закупок	R	R	R	R,W			
	Менеджер закупок	R	R	R	R,W			
Проектный офис	Начальник Проектного офиса	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
	Менеджер проекта	R	R	R	R,W			
Межбанковский расчетный центр								
Директор МБРЦ		W	R	R	R,W	W		
Заместитель Директора МБРЦ		W	R	R	R,W	W		
Заместитель главного бухгалтера		A	R	R	R,W			
Менеджер по внутренним коммуникациям		W	R	R	R,W			
Делопроизводитель		-	-	R	R,W			
Отдел итогового контроля	Начальник Отдела	W	R	R	R,W			
	Итоговый контролер	W	R	R	R,W			
Сектор по формированию документов дня и статистическим данным	Заведующий сектором-Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
	Специалист 2-категории	R	R	R	R,W			
	Специалист 2-категории	R	R	R	R,W			
Отдел Клиринговый центр платежей в национальной валюте	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел учета внутрибанковских операций	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
	Специалист 1-категории	R	R	R	R,W			
Операционное управление	Начальник операционного управления-Заместитель директора МБРЦ	W	R	R	R,W			
Бэк-офис Казначейства	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел обслуживания кредитов	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел учета операций на внутреннем рынке и ресурсов по государственным программам	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел расчетных и кассовых операций	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Ведущий специалист	W	R	R	R,W			
КАССА	Заведующий кассой	W	R	R	R,W			
	Ведущий кассир	W	R	R	R,W			
	Ведущий кассир	W	R	R	R,W			
Управление международных документарных операций	Начальник Управления	W	R	R	R,W			
Отдел импортных аккредитивов и инкассо	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел экспортных аккредитивов и гарантий	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Управление международных расчетов и организации учета валютных операций	Начальник управления - Заместитель директора МБРЦ	W	R	R	R,W			
Отдел Лоро банков-корреспондентов	Начальник Отдела	W	R	R	R,W			
	Заместитель Начальника Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
	Главный специалист	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
Отдел НОСТРО	Начальник Отдела	W	R	R	R,W			
	Главный специалист	W	R	R	R,W			
	Ведущий специалист	W	R	R	R,W			
Отдел электронных платежей по системе СВИФТ	Начальник Отдела	W	R	R	R,W	W		
	Главный специалист	W	R	R	R,W	W		
	Ведущий специалист	W	R	R	R,W	W		
Департамент управления делами								
Директор Департамента		-	R	R	R,W			
Заместитель Директора Департамента		-	R	R	R,W			
Делопроизводитель		-	R	R	R,W			
Отдел по обеспечению материальными ресурсами, бронированию авиабилетов и гостиниц	Начальник Отдела	-	R	R	R,W			
	Главный специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
	Ведущий специалист	-	R	R	R,W			
Администратор интегрированной автоматизированной банковской системы	Начальник Управления поддержки информационных систем ДИТ	R,W,A,D,P						
Администратор БИС, IBANK, Milliy (web и mobile)	Начальник отдела сопровождение дистанционного банковского обслуживания ДИТ		R,W,A,D, P					

Пользователи		ИАБС	БИС	СЭД	Файл сервер FTP	БД SWIFT	БД VISA/ Master Card	БД ЭЦП
Администратор системы электронного документоборота	Начальник отдела разработки программного обеспечения ДИТ			R,W,A,D, P				
Администратор файл-сервера	Ведущий инженер-системный администратор отдела системного программного обеспечения				R,W,A,D,P			
Администратор SWIFT	Главный инженер-системный администратор отдела системного программного обеспечения ДИТ					R,W,A,D P		
Администратор VISA/Master Card	Начальник отдела разработки и внедрения новых продуктов ДРБ						R,W,A,DP	
Администратор ЭЦП	Начальник отдела анализа и управление информационными рисками ДИББ							R,W,A,D,P

Филиал Главного управления по городу Ташкенту				
		ИАБС	БИС	Файл Сервер FTP
Управляющий		R	R	R,W
Первый Заместитель управляющего		R	R	R,W
Заместитель Управляющего по координации и исполнению Поручений Президента РУ		R,W	R	R,W
Первый Заместитель Управляющего по работе с филиалами		R,W	R	R,W
Заместитель Управляющего		R,W	R	R,W
Аппарат Главного управления	Заведующий сектором	R	R	R,W

	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
	Делопроизводитель	-	R	R,W
Сектор координации инвестиционной деятельности и развития сферы услуг	Заведующий сектором	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	R	R	R,W
Сектор развития молодежного предпринимательства	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
Центр инвестиции	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Управление кредитования	Начальник управления	R,W	R	R,W
Отдел управления и анализа кредитного портфеля	Начальник отдела - Заместитель начальника управления	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Отдел экспертизы инвестиционных проектов	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
Отдел экспертизы кредитов малого бизнеса	Начальник отдела	R	R	R,W
	Ведущий специалист	R	R	R,W
Отдел мониторинга и контроля за исполнением социальных программ и агросектора	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Отдел валютных операций	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Специалист 1-категории	W	R	R,W

Управление денежного обращения, розницы и контроля кассовых операций	Начальник управления	R,W	R	R,W
Отдел денежного обращения	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
Отдел по работе с пластиковыми карточками	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор кассовых операций	Заведующий сектором	W	R	R,W
	Главный специалист	W	R	R,W
Отдел розничных операций и мониторинга кредитования физических лиц	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел конверсионных операций и координации деятельности валюто-обменных пунктов	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел мониторинга и работы с проблемными кредитами	Начальник отдела	R	R	R,W
Сектор мониторинга кредитов	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Сектор взыскания проблемных кредитов	Заведующий сектором	R,W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W

Управление бухгалтерского учета, отчетности и экономического анализа	Начальник Управления - Главный бухгалтер	R,W	R	R,W
Отдел бухгалтерского учета и финансовой отчетности	Начальник отдела - Заместитель главного бухгалтера	W,R	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел планирования бюджета и его исполнения	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
Сектор управления ликвидности и экономического анализа	Заведующий сектором	R	R	R,W
	Главный специалист по управлению ликвидностью	R	R	R,W
Отдел учетно-расчетных операций	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел итогового контроля	Начальник Отдела	R	R	R,W
	Итоговый контролер по _____ филиалу	R	R	R,W
Отдел внутреннего контроля	Начальник Отдела	R	R	R,W
	Итоговый контролер по _____ филиалу	R	R	R,W

Сектор оценки и мониторинга залогового обеспечения	Заведующий сектором	R	R	R,W
Управление проектного финансирования	Управление проектного финансирования	R	R	R,W
Отдел экспертизы, мониторинга и финансирования инвестиционных проектов	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1-категории	R	R	R,W
Отдел финансирования инвестиционных проектов в малом бизнесе	Начальник отдела	R,W	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1-категории	R	R	R,W
Отдел юридической службы	Начальник отдела	-	R	R,W
	Главный юрисконсульт	-	R	R,W
	Главный юрисконсульт	-	R	R,W
	Главный юрисконсульт	-	R	R,W
	Главный юрисконсульт по _____ филиалу	-	R	R,W
Отдел по безопасности, режиму и защите информации	Начальник отдела	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист по комплаенс контролю и противодействию коррупции	-	R	R,W
1 Сектор	Главный специалист	-	R	R,W
Отдел по работе с персоналом	Начальник отдела	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W

	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Главный специалист	-	R	R,W
	Ведущий специалист	-	R	R,W
Администрация	Главный специалист по делопроизводству	-	R	R,W
	Ведущий специалист по архивному делу	-	R	R,W
	Секретарь	-	R	R,W
	Секретарь	-	R	R,W
	Курьер	-	R	R,W
Отдел автоматизации и компьютеризации	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Хозяйственный отдел	Начальник отдела	R	R	R,W
	Заместитель начальника отдела	-	R	R,W
	Главный специалист по капитальному строительству и эксплуатации объектов	-	R	R,W
	Сантехник	-	R	R,W
	Электрик	-	R	R,W
	Водитель	-	R	R,W
	Архивариус-переплетчик	-	R	R,W
	Разнорабочий	-	R	R,W

	Уборщица	-	R	R,W
Сектор снабжения товаро-материальных ценностей	Заведующий сектором	-	R	R,W
	Главный специалист	-	R	R,W
	Заведующий складом	-	R	R,W
	Разнорабочий	-	R	R,W

Операционное управление при Главном управлении АО «НБ ВЭД РУ» по городу Ташкенту				
		ИАБС	БИС	Файл Сервер FTP
Управляющий		R	R	R,W
Заместитель Управляющего		R,W	R	R,W
Главный бухгалтер		R,W	R	R,W
Старший менеджер по развитию сети и сервиса банка			R	R,W
Группа Корпоративного обслуживания	Первый Заместитель Управляющего-Начальник Группы	W	R	R,W
Отдел обслуживания юридических лиц	Заместитель главного бухгалтера-Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор денежного обращения и кассовых операций	Главный специалист	W	R	R,W
Отдел валютных операций	Начальник отдела	W	R	R,W
	Заместитель начальника отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W

	Специалист 2 категории	W	R	R,W
Сектор мониторинга и контроля за исполнением социальных программ и агросектора	Заведующий сектором	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1 категории	R	R	R,W
Отдел кредитования юридических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор микрокредитования юридических лиц	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Группа Розничного обслуживания	Заместитель Управляющего-Начальник Группы	W	R	R,W
Отдел розничных операций	Заместитель главного бухгалтера-Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел кредитования физических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел обслуживания и выпуска пластиковых карточек	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W

	Специалист 2 категории	W	R	R,W
Сектор конверсионных и валютно-обменных операций	Главный специалист	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
	Главный специалист по безопасности и режиму	W	R	R,W

Главный операционный филиал по городу Ташкенту

Группа контроля и поддержки бизнеса	Секретарь	ИАБС	БИС	Файл Сервер FTP
Управляющий	Секретарь-ресепшн	R	R	R,W
Заместитель Управляющего	Инспектор по пропускному режиму	R,W	R	R,W
Главный бухгалтер				
Отдел учетно-расчетных операций	Главный специалист	W	R	R,W
Старший менеджер по развитию сети и сервиса банка	Начальник отдела	R,W	R	R,W
Отдел мониторинга выданных кредитов	Первый Заместитель Управляющего-			
Группа Корпоративного обслуживания	Главный специалист Начальник Группы	R,W	R	R,W
	Ведущий специалист	R	R	R,W
	Заместитель главного бухгалтера-			
Сектор автоматиазции и компьютеризации	Заведующий сектором Начальник отдела	W	R	R,W
Отдел обслуживания юридических лиц	Главный специалист	W	R	R,W
	Начальник отдела			
	Ведущий специалист	W	R	R,W
Отдел кассовых операций	Заведующий кассой Специалист 1 категории	W	R	R,W
Сектор денежного обращения и кассовых операций	Кассир-контролер	W	R	R,W
	Главный специалист	W	R	R,W
	Кассир-эксперт	W	R	R,W
Сектор мониторинга и контроля за исполнением социальных программ и агросектора	Заведующий сектором	R	R	R,W
	Заведующий сектором Ведущий специалист	R	R	R,W
	Водитель Специалист 1 категории	R	R	R,W
	Архивариус-переплетчик	R	R	R,W
Хозяйственный сектор	Заведующий сектором	W	R	R,W
	Садовник Главный специалист	W	R	R,W
Отдел валютных операций	Уборщица			
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
	Курьер			

Отдел кредитования юридических лиц	Начальник отдела	R,W	R	R,W
Сектор кредитования корпоративных клиентов	Заведующий сектором	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор кредитования МСБ	Заведующий сектором	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор координации инвестиционной деятельности и развития сферы услуг	Заведующий сектором	-	R	R,W
	Главный специалист	-	R	R,W
	Ведущий специалист	-	R	R,W
Группа Розничного обслуживания	Заместитель Управляющего-Начальник Группы	R,W	R	R,W
Отдел розничных операций	Заместитель главного бухгалтера-Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел кредитования физических лиц	Начальник отдела	W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор кредитования населения	Заведующий сектором	R,W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор кредитования розницы	Заведующий сектором	R,W	R	R,W
	Специалист 1 категории	R	R	R,W
Отдел выпуска и обслуживания пластиковых карточек	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W

	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор конверсионных и валютно-обменных операций	Заведующий сектором	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Группа контроля и поддержки бизнеса	Главный специалист по безопасности и режиму	R	R	R,W
	Секретарь	R	-	R,W
	Секретарь-ресепшн	R	-	R,W
	Инспектор по пропускному режиму	R	-	R,W
Отдел учетно-расчетных операций	Главный специалист	W	R	R,W
Отдел мониторинга выданных кредитов	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Сектор автоматиазции и компьютеризации	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
КАССА	Заведующий кассой	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Хозяйственный сектор	Заведующий сектором	-	-	-
	Электрик	-	-	-
	Сантехник	-	-	-
	Водитель	-	-	-
	Архивариус-переплетчик	-	-	-
	Садовник	-	-	-
	Уборщица	-	-	-

	Курьер	-	-	-

Районные филиалы города Ташкента				
		ИАБС	БИС	Файл Сервер FTP
Управляющий		R	R	R,W
Главный бухгалтер		R,W	R	R,W
Старший менеджер по развитию сети и сервиса банка			R	R,W
Группа Корпоративного обслуживания	Первый Заместитель Управляющего-Начальник Группы	R,W	R	R,W
Отдел обслуживания юридических лиц	Заместитель главного бухгалтера-Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор денежного обращения и кассовых операций	Главный специалист	W	R	R,W
Сектор/Отдел валютных операций	Заведующий сектором	W	R	R,W
	Главный специалист	W	R	R,W
Сектор мониторинга и контроля за исполнением социальных программ и агросектора	Заведующий сектором	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1 категории	R	R	R,W
Отдел кредитования юридических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор координации инвестиционной деятельности и развития сферы услуг	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W

	Ведущий специалист	R	R	R,W
Группа Розничного обслуживания	Заместитель Управляющего-Начальник Группы	R	R	R,W
Отдел розничных операций	Заместитель главного бухгалтера-Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел кредитования физических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел выпуска и обслуживания пластиковых карточек	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор конверсионных и валютно-обменных операций	Главный специалист	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Группа контроля и поддержки бизнеса	Главный специалист по безопасности и режиму	W	R	R,W
	Секретарь	-	-	R,W
	Секретарь-ресепшн	-	-	R,W
	Инспектор по пропускному режиму	R	R	R,W
Отдел учетно-расчетных операций	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W

	Специалист 1 категории	W	R	R,W
Отдел мониторинга выданных кредитов	Начальник отдела	R,W	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Сектор автоматиазции и компьютеризации	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
КАССА	Заведующий кассой	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Хозяйственный сектор	Заведующий сектором	-	-	-
	Электрик	-	-	-
	Водитель	-	-	-
	Архивариус-переплетчик	-	-	-
	Садовник	-	-	-
	Уборщица	-	-	-
	Курьер	-	-	-

Областные филиалы				
		ИАБС	БИС	Файл Сервер FTP
Управляющий		R	R	R,W
Первый Заместитель управляющего		R,W	R	R,W
Заместитель управляющего		R, W	R	R,W
Старший менеджер по развитию сети и сервиса банка		-	R	R,W
Главный бухгалтер		R, W	R	R,W
Отдел денежного обращения, розницы и контроля кассовых операций	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W

	Главный специалист по управлению ликвидности	W	R	R,W
Отдел кредитования	Начальник отдела	R, W	R	R,W
	Главный специалист	W	R	R,W
	Главный специалист по координации и контролю строительства сельского жилья	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел мониторинга и контроля за исполнением социальных программ и агросектора	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1 категории	R	R	R,W
Отдел по работе с проблемными кредитами	Заместитель Управляющего - Начальник отдела	R, W	R	R,W
	Главный специалист	R, W	R	R,W
	Ведущий специалист	R, W	R	R,W
Сектор координации инвестиционной деятельности и развития сферы услуг	Заведующий сектором	R, W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор развития молодежного предпринимательства	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
Отдел итогового контроля	Начальник Отдела	R	R	R,W
	Итоговый контролер	R	R	R,W
	Итоговый контролер по ___ филиалу	R	R	R,W
Отдел внутреннего контроля	Начальник Отдела	R	R	R,W
	Compliance office	R	R	R,W
	Начальник Отдела	R	R	R,W

Отдел по безопасности, режиму и защите информации	Главный специалист	R	R	R,W
	Главный специалист по комплаенс контролю и противодействию коррупции	R	R	R,W
	Инспектор по пропускному режиму	-	R	R,W
Юридический отдел	Начальник отдела	-	R	R,W
	Главный юрисконсульт	-	R	R,W
	Главный юрисконсульт по ____ филиалу	-	R	R,W
Сектор по работе с персоналом	Заведующий сектором	-	R	R,W
	Главный специалист	-	R	R,W
	Ведущий специалист	-	R	R,W
ОПЕРАЦИОННЫЙ ОТДЕЛ	Начальник Операционного отдела	R	R	R,W
Отдел обслуживания юридических лиц	Заместитель главного бухгалтера - Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Отдел валютных операций	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел кредитования юридических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист I категории	W	R	R,W
Сектор кредитования сельского строительства	Заведующий сектором	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W

Сектор кредитования МСБ	Заведующий сектором	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Минибанк	Главный специалист	W	R	R,W
	Ведущий специалист	R,W	R	R,W
Отдел обслуживания физических лиц	Заместитель главного бухгалтера - Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
	Специалист 2 категории	W	R	R,W
Сектор/Отдел кредитования физических лиц	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел выпуска и обслуживания пластиковых карточек	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	R,W	R	R,W
Сектор валютно-обменных операций	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Сектор по работе с обращениями юридически и физических лиц	Заведующий сектором	R,W	R	R,W
Группа контроля и поддержки бизнеса	Специалист 2 категории по документации и архиву	R	R	R,W
	Секретарь	-	R	R,W
	Секретарь-ресепшн	-	R	R,W
Отдел учетно-расчетных операций	Начальник отдела	R,W	R	R,W

	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел мониторинга выданных кредитов	Начальник отдела	R	R	R,W
	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Сектор автоматизации и компьютеризации	Заведующий сектором	R	R	R,W
	Главный специалист	R	R	R,W
КАССА	Заведующий кассой	R,W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Хозяйственный отдел	Начальник хозяйственного отдела	-	-	-
	Главный специалист по капитальному строительству и эксплуатации объектов	-	-	-
	Главный энергетик	-	-	-
	Заведующий складом	-	-	-
	Электрик	-	-	-
	Водитель	-	-	-
	Архивариус-переплетчик	-	-	-
	Уборщица	-	-	-
	Курьер	-	-	-

Районные филиалы областей				
		ИАБС	БИС	Файл Сервер FTP
Управляющий		R	R	R,W

Главный бухгалтер		R,W	R	R,W
Заместитель главного бухгалтера		R,W	R	R,W
Главный специалист по автоматизации		R	R	R,W
Специалист 2-категории по учету кадров и архиву		R	R	R,W
Секретарь-ресепшн		-	-	R,W
Отдел обслуживания юридических лиц	Первый Заместитель управляющего - Начальник отдела	R,W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор кредитования юридических лиц	Главный специалист	R,W	R	R,W
	Ведущий специалист	W	R	R,W
Сектор мониторинга и контроля за исполнением социальных программ и агросектора	Заведующий сектором	R	R	R,W
	Ведущий специалист	R	R	R,W
	Специалист 1 категории	R	R	R,W
Сектор микрокредитования	Ведущий специалист	W	R	R,W
Сектор кредитования сельского строительства	Заведующий сектором	W	R	R,W
	Главный специалист	W	R	R,W
Сектор микрокредитования	Ведущий специалист	W	R	R,W
Сектор валютных операций	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел розничных операций	Заместитель Управляющего-Начальник отдела	R,W	R	R,W
	Ведущий специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W
Сектор кредитования физических лиц	Главный специалист	W	R	R,W
	Специалист 1 категории	W	R	R,W

Отдел конверсионных операций и обслуживания пластиковых карточек	Начальник отдела	W	R	R,W
	Главный специалист	W	R	R,W
Сектор обменных операций	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
КАССА	Заведующий кассой	W	R	R,W
	Кассир-контролер	W	R	R,W
	Кассир-эксперт	W	R	R,W
Отдел учетно-расчетных операций	Заместитель главного бухгалтера - начальник отдела	R,W	R	R,W
Отдел мониторинга выданных кредитов	Начальник отдела	R,W	R	R,W
	Главный специалист	W	R	R,W
Хозяйственный сектор	Заведующий сектором	-	-	-
	Машинист широкого профиля	-	-	-
	Электрик	-	-	-
	Дворник	-	-	-
	Уборщица	-	-	-
Сектор координации инвестиционной деятельности и развития сферы услуг	Заведующий сектором	-	-	-
	Главный специалист	-	-	-
	Ведущий специалист	-	-	-

Центр оказания банковских услуг				
		ИАБС	БИС	Файл Сервер FTP
Заведующий центром		R,W	R	R,W
Отдел по безопасности, режиму и защите информации	Главный специалист	R	R	R,W

Отдел обслуживания юридических лиц	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел обслуживания физических лиц	Главный специалист	W	R	R,W
	Ведущий специалист	W	R	R,W
Отдел по работе с проблемными активами	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Отдел мониторинга выданных кредитов	Главный специалист	R	R	R,W
	Ведущий специалист	R	R	R,W
Касса	Кассир-эксперт	W	R	R,W

Приложение №11
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-1 27.12.2021г

Перечень разрешенного к использованию программного обеспечения

1. Установка и обновление операционной системы и её компонентов, программного обеспечения на рабочих станциях и серверах в головном офисе осуществляется Отделом системного программного обеспечения ДИТ, а в областных и районных филиалах, минибанках – Секторами автоматизации, компьютеризации и внедрения ИКТ. Самостоятельная установка пользователями операционной системы и программного обеспечения не допускается.

2. На рабочих станциях сотрудников АО «Узнацбанк» устанавливаются пользовательские права.

Администраторские права устанавливаются на отдельных рабочих станциях администраторов в случае необходимости (используемые для обслуживания серверов и оборудования) по разрешению директора ДИТ или директора ДИББ.

3. Перечень разрешенного к использованию программного обеспечения приведен в Таблице №1.

Таблица №1

Перечень разрешенного к использованию программного обеспечения

1. Программы, устанавливаемые на рабочие станции	
1. Операционные системы	
1.1.	Операционные системы семейства Windows компании Microsoft, включая их обновления (критические, по безопасности, улучшающие функциональность и исключающие ошибки в программах)
2. Офисные программы	
2.1.	Офисные программы семейства Microsoft Office,
3. Программные продукты сторонних информационных систем	
3.1.	Информационный поисковая система «Norma»
4. Электронная почта	
4.1.	Microsoft Outlook
5. Электронный документооборот	
5.1.	Программа системы электронного документооборота АО «Узнацбанк» “Personal”
5.2.	LotusNotes
5.3.	Защищенная электронная почта EXAT
6. Программные продукты для шифрации и дешифрации информации	
6.1.	Connection Manager Client, Agro Crypt, SFiT Client, Styx Client
7. Антивирусные программы	

7.1.	Антивирусные продукты ESET
7.2.	Утилиты для удаления вирусов
8. Файловые менеджеры	
8.1.	Total Commander
8.2.	FarManager
9. Архиваторы	
9.1.	Arj, Rar, Zip
10. Программы для работы с PDF файлами	
10.1.	Программа для просмотра файлов PDF: Adobe Acrobat reader, Foxit Reader, ABBYY FineReader
10.2.	Программа для редактирования файлов PDF: AdobeProfessional, NitroPro, ABBYY FineReader
11. Видео и аудио плееры	
11.1.	Windows Media Player, AIMP, Pot player
12. USB-токен безопасности	
12.1.	SafeNetIkey 1000, RainbowiKey 100
13. Специальное программное обеспечение	
13.1	Не имеются
14. Интернет браузеры (обозреватели)	
14.1.	Google Chrome, Mozilla FireFox, Internet Explorer, Microsoft Edge
15. Драйверы и утилиты	
15.1.	Программы и утилиты производства компании Sun
15.2.	Программы и утилиты производства компании Microsoft
16. Программные продукты информационных систем собственной разработки	
16.1.	Программный комплекс ОДБ NBS+PAYMENT
16.2.	Программный комплекс I-BANK
16.3.	Программный комплекс BIS
16.4.	Информационно интерактивная система “Personal”
2. Программы, устанавливаемые на сервера	
1. Операционные системы	
1.1.	Операционные системы семейства Windows Server компании Microsoft, включая их обновления (критические, по безопасности, улучшающие функциональность и исключающие ошибки в программах)
1.2.	Операционные системы семейства Linux и Unix, включая их обновления
2. Антивирусные программы	
2.1.	Антивирусные продукты ESET
3. Архиваторы	
3.1	Rar
4. Файловые менеджеры	
4.1.	Total Commander

4. Установка иного необходимого программного обеспечения на отдельные рабочие станции, в том числе на серверах, осуществляется строго на основании аргументированной заявки на директора ДИТ с обязательным согласованием с ДИББ.

5. ДИТ имеет право допустить к использованию иное аналогичное программное обеспечение в случаях прекращения выпуска разработчиками обновлений или поддержки программ, а также появления новых программ, превосходящих по функционалу или имеющих меньшую стоимость по сравнению с указанными в перечне.

6. Изменения и дополнения в Перечень разрешенного к использованию программного обеспечения могут вноситься ответственными подразделениями по согласованию с ДИТ и ДИББ, последующим утверждением Перечня заместителем председателя правления, курирующим подразделение ДИББ.

Приложение №12
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-1 27.12.2021г

Инструкция по работе с сетью Интернет и корпоративной электронной почтой

1. Основные положения

1.1 Настоящая Инструкция устанавливает порядок и требования к использованию сети Интернет (TAS-IX) и работе с корпоративной электронной почтой сотрудниками АО «Узнацбанк».

1.2 Доступ к сети Интернет предоставляется ограниченному кругу сотрудников, являющихся руководством правления АО «Узнацбанк», областных и районных филиалов, а также определенным работниками головного офиса, областных и районных филиалов в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

1.3 Доступ сотрудников АО «Узнацбанк» к сети Интернет организуется через единый прокси-сервер, который установлен в основном ЦОД АО «Узнацбанк» и обслуживается УИБ ДИББ.

Корпоративная сеть АО «Узнацбанк» должна быть физически связана с Интернет (сетями операторов передачи данных, предоставляющих доступ к сети Интернет и TAS-IX) через отдельный маршрутизатор и отдельный межсетевой экран.

1.4 Доступ к сети Интернет сотрудникам АО «Узнацбанк» предоставляется исходя из служебной необходимости, на основании служебной записки на имя директора ДИББ от имени руководителя подразделения.

Без согласования ДИББ запрещена самостоятельная организация дополнительных точек доступа в Интернет.

1.5 Перед работой в сети Интернет сотрудник АО «Узнацбанк» обязан подписать обязательства при работе в сети Интернет, которые определены в Порядке предоставления доступа к сети Интернет работникам АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

1.6 Доступ к сети Интернет сотрудникам АО «Узнацбанк» предоставляется УИБ ДИББ, которое также обеспечивает контроль за надлежащим исполнением настоящей Инструкции при пользовании сотрудниками банка сетью Интернет.

1.7 Доступ к сети Интернет осуществляется с рабочей станции. Ответственность за действия на рабочей станции другого человека, несет пользователь рабочей станции, с которого совершено это действие.

Запрещается организовывать и предоставлять подключение к сети Интернет рабочих станций и серверов, имеющих доступ или используемых в ИАБС. Контроль выполнения данного требования обеспечивается ДИББ.

1.8 В АО «Узнацбанк» создает собственный сервер внутренней системы электронной почты в корпоративной сети банка.

Корпоративная электронная почта предоставляется сотрудникам АО «Узнацбанк» при подключении их к единой ЛВС АО «Узнацбанк». Персональный адрес корпоративной электронной почты предоставляется сотруднику банка вместе с реквизитами доступа к единой ЛВС АО «Узнацбанк» (учетной записи).

Подключение сотрудников к корпоративной электронной почте обеспечивается Отделом ДИТ.

1.9 Исходя из служебной необходимости, отдельным сотрудникам АО «Узнацбанк» предоставляется сервис внешней электронной почты оператора EastTelecom.

Список сотрудников АО «Узнацбанк», получающих доступ к внешней электронной почте, определяется ДИТ.

1.10 Корпоративная электронная почта и внешняя электронная почта используется для обмена служебной информацией в виде текстовых сообщений или документов в электронном виде.

Запрещается передача любой конфиденциальной информации по корпоративной и внешней электронной почте в незашифрованном виде без применения ЭЦП, т.е. без обеспечения её конфиденциальности и целостности.

1.11 Право использование систем мгновенного обмена сообщениями (мессенджеры) предоставляется сотрудникам банка, у которых имеется производственная потребность в их применении для выполнения своих служебных обязанностей. Перечень этих сотрудников определяется на основании служебной записки директором ДИББ.

1.12 Запрещается передача служебной (деловой), банковской и конфиденциальной информации через системы мгновенного обмена сообщениями, а также через другие системы обмена информации в сети Интернет (Интернет-почта, социальные сети, онлайн-видеоконференции и т.д.).

1.13 Любая электронная информация, подготовленная или полученная АО «Узнацбанк» для отправки через Интернет и электронную почту, должна проверяться с помощью антивирусного программного обеспечения. Данные, полученные по электронной почте, следует проверять в специальной зоне на наличие повреждений (система Sandbox).

2. Основные требования к пользователям сети Интернет

2.1 При пользовании сетью Интернет необходимо:

- соблюдать требования настоящей Инструкции;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность сотрудников УИБ ДИББ, Отделов по безопасности, режиму и защите информации областных филиалов и главных специалистов по безопасности, режиму и защите информации районных филиалов о любых фактах нарушения требований настоящей Инструкции;

- хранить свои идентификационные данные (логины, пароли, криптографические ключи и т.п.) в тайне, не передавать или не сообщать идентификационные данные третьим лицам.

2.2 Сотрудники банка имеют право пользоваться сетью Интернет в целях:

- распространения общедоступной информации о деятельности АО «Узнацбанк» и оказываемых им банковских услугах;
- освещения новостной информации АО «Узнацбанк» в сети Интернет, а также сведений о публичных мероприятиях АО «Узнацбанк»;
- осуществления взаимодействия и взаимоотношений с клиентами банка, ознакомления их с порядком и правилами получения банковских услуг АО «Узнацбанк»;
- ознакомления с общественно-политической и социально-экономической жизнью Узбекистана и получения информации о последних событиях в республике и мире;
- проведения маркетинговых исследований в банковской сфере, изучение внутреннего банковского рынка;
- поддержания официального веб-сайта АО «Узнацбанк» и своевременного заполнения его актуальной информацией;
- получения информации с разных источников в сети Интернет, требуемой для осуществления деятельности сотрудниками АО «Узнацбанк»;
- изучения зарубежного опыта и международных тенденций в банковской сфере;
- обмена информацией с зарубежными, международными и национальными организациями в рамках взаимного сотрудничества и обмена опытом;
- пользования онлайн-услугами сотрудниками АО «Узнацбанк», в частности приобретение билетов, бронирование гостиниц, получение виз и т.д.
- решения организационные вопросов, связанных с командировками, приемами зарубежных представителей, проведением иных мероприятий, осуществляемых АО «Узнацбанк»;
- своевременного обновления программных средств и др.

2.3 При пользовании сетью Интернет запрещено:

- использовать предоставленный доступ в сеть Интернет в личных целях;
- передавать конфиденциальную информацию не в зашифрованном виде;
- использовать специализированные аппаратные и программные средства, позволяющие сотрудникам получить несанкционированный доступ к сети Интернет;
- использовать внешние прокси-сервера при работе в сети Интернете;
- публиковать корпоративные электронные адреса АО «Узнацбанк» на досках объявлений, в конференциях и гостевых книгах;
- использовать некорпоративную электронную почту, социальные сети и системы мгновенных сообщений для рассылки служебной и конфиденциальной информации;
- передавать учетные данные пользователей и паролей;
- проводить незаконные операции и совершать иные действия в сети Интернет, противоречащие законодательству, а также настоящей Инструкции.

3. Получение и распространение информации с помощью сети Интернет

3.1 Сотрудники АО «Узнацбанк» получают доступ к сети Интернет со своих рабочих станций. Сотрудники получают доступ к сети Интернет в целях получения и распространения информации.

3.2 Сотрудники АО «Узнацбанк» могут получать с сети Интернет любую информацию, необходимую для выполнения своих служебных обязанностей путем обращения на информационные ресурсы в сети Интернет через поисковые системы либо набором URL-адреса.

3.3 Сотрудники АО «Узнацбанк» имеют право распространять информацию в сети Интернет в целях:

- освещения общедоступной информации о деятельности АО «Узнацбанк», его подразделений и о своих банковских услугах;
- распространение новостной информации и сведений о публичных мероприятиях АО «Узнацбанк»;
- доведение до клиентов банков требуемой информации о порядке и правилах оказания своих услуг, а также о местах их получения;
- распространение информации о вакантных местах в АО «Узнацбанк»;
- предоставление контактных данных и иной информации для взаимодействия с АО «Узнацбанк».

3.4 Право распространение вышеуказанной информации предоставляется сотрудникам АО «Узнацбанк» в соответствии с их служебными обязанностями.

3.5 При распространении информации в сети Интернет сотрудники АО «Узнацбанк» должны выполнять следующие требования:

- публиковать достоверную, полною и объективную информацию;
- при публикации материалов, в том числе выражающих личное мнение, придерживаться исключительно своей сферы должностных обязанностей;
- помнить, что публикации формируют мнение и впечатление об АО «Узнацбанк»;
- соблюдать требования законодательства по защите прав потребителей;
- осознавать всю полноту ответственности за публикуемые материалы;
- соблюдать и уважать права третьих лиц на результаты интеллектуальной деятельности и средства индивидуализации;
- избегать конфликтов, неконструктивных споров с другими пользователями Интернет.

3.6 Запрещается публиковать, загружать и распространять материалы, содержащие:

- конфиденциальную информацию, а также информацию, составляющую коммерческую и банковскую тайну, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с ДИББ заранее;
- информацию, полностью или частично, защищенную авторскими или другими правами, без разрешения владельца;

- вредоносное программное обеспечение, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому программному обеспечению и программному обеспечению для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

- угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д;

- прочую служебную информацию.

3.7 Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного программного обеспечения.

3.8 Запрещается:

- посещать ресурсы трансляции потокового видео и аудио, создающих большую загрузку сети и мешающих нормальной работе остальных сотрудников банка;

- посещать и использовать эротико-порнографические ресурсы сети Интернет, ресурсы националистических организаций, ресурсов, пропагандирующие насилие и терроризм.

4. Контроль использования ресурсов сети Интернет

4.1 УИБ ДИББ имеет право блокировать или ограничивать доступ сотрудников к определенным Интернет-ресурсам, противоречащим Политике информационной безопасности и содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и национальным законодательством.

Ограничение доступа к определенным Интернет-ресурсам осуществляется путем фильтрации запросов и трафика на прокси-сервере.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется в соответствии с требованиями Порядка предоставления доступа к сети Интернет работникам АО «Узнацбанка».

Доступ сотрудников банка должен ограничиваться к следующим Интернет-ресурсам:

- внешняя электронная почта (mail.ru, mail.yandex.ru, gmail.com и др.);
- мессенджеры и интернет-пейджеры;
- социальные сети.

Ограничение доступа к указанным Интернет-ресурсам направлено на исключение использования этих каналов для утечки конфиденциальной информации сотрудниками банка.

Список Интернет-ресурсов, доступ к которым ограничивается для сотрудников банка, определяется и ведется УИБ ДИББ.

4.2 Доступ сотрудников АО «Узнацбанка» к ресурсам также ограничивается в соответствии с требованиями разработанной Матрицы доступа к информационным ресурсам, а также в соответствии с установленными обязанностями (деятельностью) сотрудника в сети Интернет и на основании списка сотрудников, которым предоставлен доступ к сети Интернет.

4.3 Работа сотрудников банка в сети Интернет отслеживается с помощью специального программного обеспечения (далее - система контроля Интернет-доступа). На основе электронной записи логов проводится анализ по следующим параметрам:

- перечень посещаемых Интернет-ресурсов;
- объём использованного трафика.

Система контроля Интернет-доступа должна автоматически вести электронную запись пользования сотрудниками банка сети Интернет, содержащую логин пользователя, дату и время посещения Интернет-ресурса, его адреса и загруженного содержимого. Электронная запись о посещенных Интернет-ресурсах должна храниться не менее трех месяцев для дальнейшего их анализа со стороны УИБ ДИББ.

4.4 УИБ ДИББ имеет право производить выборочные и полные проверки по целевому использованию сети Интернет сотрудниками банка.

4.5 Информация о посещаемых сотрудниками Интернет-ресурсах протоколируется, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководству АО «Узнацбанка» для контроля.

4.6 По результатам выборочных и полных проверок по целевому использованию сети Интернет выявляются наиболее злостные нарушители настоящей Инструкции.

4.7 Факты нецелевого использования фиксируются в виде «Акта о нецелевом использовании Интернета» УИБ ДИББ.

По выявленному факту нецелевого использования Интернета со злостного нарушителя снимаются письменные показания в виде объяснительной записки.

Акт о нецелевом использовании Интернета вносится директору ДИББ.

4.8 При подозрении сотрудника банка в нецелевом использовании Интернета инициируется служебная проверка.

5. Правила пользования корпоративной и внешней электронной почтой

5.1 При работе с корпоративной и внешней электронной почтой сотрудник банка должен учитывать следующие принципиальные положения:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передача конфиденциальной информации разрешается только по системе защищенной электронной почты E-xat.

5.2 К размеру почтового ящика пользователя и объему передаваемой информации устанавливается ограничение. В случае превышения объема хранимой или передаваемой информации установленного лимита доступ к почте блокируется. При блокировании доступа к почте выдается сообщение о превышении лимита объема его почтового ящика и требуется очистка почтового ящика пользователя.

5.3 Пользователям корпоративной и внешней электронной почты запрещается:

- использование корпоративной электронной почты для частной переписки, в коммерческих целях;
- отправлять и передавать конфиденциальную информацию не в зашифрованном виде;
- пересылать по корпоративной электронной почте или с помощью других средств электронной связи информацию политического, религиозного, антигуманного характера, а также непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы, отображать и хранить их. В случае появления информации подобного характера пользователь должен немедленно сообщить об этом своему непосредственному руководителю;
- производить рассылку материалов рекламного (непрофильного) и развлекательного характера;
- производить массовую рассылку писем непроизводственного характера;
- производить рассылку вредоносных программ или файлов, зараженных вирусами;
- предоставлять, кому бы то ни было пароль доступа к своему почтовому ящику;
- пересылать по электронной почте пароли к каким бы то ни было информационным системам и ресурсам АО «Узнацбанк».

5.4 Содержание передаваемого сообщения электронной почты и других электронных документов должно быть кратким, лаконичным и точным.

5.5 Категорически запрещается:

- использование несанкционированных внешних почтовых сервисов вне доменной зоны «.UZ» для переписки и обмена служебной и конфиденциальной информацией;
- передача по корпоративной и внешней электронной почте конфиденциальной информации.

6. Ответственность

6.1 Сотрудники банка несут персональную ответственность за нарушение настоящей Инструкции и требований Порядка предоставления доступа к сети Интернет работникам АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

6.2 Нарушение правил пользования сетью Интернет, корпоративной и внешней электронной почты, установленных настоящей Инструкцией, влечёт за собой наложение дисциплинарной ответственности в соответствии с внутренним трудовым распорядком и трудовым законодательством Республики Узбекистан.

6.3 УИБ ДИББ несет ответственность за обеспечение контроля выполнения настоящей Инструкции сотрудниками банка.

Приложение №13
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 27.12.2021г

Порядок управления информационными активами

1. Основные положения

1.1 Настоящий порядок устанавливает требования по формированию Реестра информационных ресурсов АО «Узнацбанк» (далее – Реестр), порядок инвентаризации, классификации и маркировки информации и информационных ресурсов.

1.2 Действие Порядка управления информационными активами распространяется на информационные активы, принадлежащие АО «Узнацбанк» и используемые сотрудниками банка.

1.3 УИБ ДИББ является ответственным за составление и поддержание в актуальном состоянии Реестра по форме, согласно приложению к настоящему Порядку.

В приведенный в приложении к настоящему Порядку Реестр могут вноситься изменения и дополнения по мере появления новых информационных ресурсов.

1.4 Основными информационными ресурсами (активами) являются:

- служебная (деловая) информация АО «Узнацбанк»;
- информация, составляющая коммерческую тайну АО «Узнацбанк», его клиентов и партнеров, контрагентов, с которыми имеются соглашения и договора;
- информация, составляющая банковскую тайну в банковской системе АО «Узнацбанк»;
- персональные данные сотрудников АО «Узнацбанк» и его клиентов;
- базы данных информационных систем и их резервные копии;
- файлы FTP-сервера;
- официальный веб-сайт АО «Узнацбанк» и другие.

1.5 В Реестре должна быть установлена классификация информационных ресурсов, согласно классификации хранящейся в ней информации.

2. Ответственность за информационные активы

2.1 Владельцы информационного ресурса (актива) и УИБ ДИББ являются ответственным за:

- обеспечение доступности, конфиденциальности и целостности информационного актива;
- обеспечение соответствующей классификации информационного актива;
- разграничение полномочий и управление доступом сотрудников АО «Узнацбанк» к информационному активу.

2.2 Владелец информационного ресурса (актива) несет ответственность за обеспечение прав доступа к информационному активу и контроль за этим доступом.

2.3 Для каждого информационного ресурса (актива) на основании его ценности устанавливается уровень защиты. Уровень защиты информационного актива определяется УИБ ДИББ по согласованию с владельцем информационного актива.

2.4 Ответственность за составление и поддержание в актуальном состоянии Реестра, а также установление требований к обеспечению их конфиденциальности, целостности и доступности в зависимости от категории информационных ресурсов возлагается на УИБ ДИББ.

2.5 Ответственность за обеспечение информационной безопасности информационных ресурсов возлагается на владельцев данных ресурсов, а контроль за должным обеспечением информационной безопасности возлагается на УИБ ДИББ.

3. Владение информационными активами

3.1 Владельцем информационного актива является подразделение АО «Узнацбанк», которое осуществляет формирование и ведение (информационное обеспечение) информационного актива.

3.2 Владельцев (подразделения АО «Узнацбанк») всех основных информационных ресурсов (активов) должны идентифицироваться и указываться в Реестре.

3.3 За владельцем информационного актива АО «Узнацбанк» закрепляются вся информация актива, процессы обработки информации и связанные с ним средства обработки информации и приложения.

3.4 Право владения информационным активом не может быть делегировано самим владельцев другому подразделению. Данное делегирование производится в соответствии с решением руководства правления АО «Узнацбанк».

4. Допустимое использование информационных активов

4.1 Доступ к информационным активам получают те сотрудники АО «Узнацбанк», которые имеют такой доступ.

4.2 Доступ к информационным активам предоставляется сотрудникам для пользования информацией, а также для формирования (информационного обеспечения) информационного актива. Указанный доступ организуется в соответствии с Матрицей доступа, которая формируется в соответствии с Правилами разработки матрицы, приведенной в приложении №10 к Политике информационной безопасности.

4.3 Сотрудники АО «Узнацбанк» обязаны использовать информационные активы (ресурсы) по их назначению.

4.4 Пользователи информационных активов (ресурсов) должны указываться в Реестре.

4.5 Правила доступа и пользования информационными активами должны определяться исходя из уровня их конфиденциальности, целостности и доступности.

4.6 Доступ к информационным активам категории «ДСП» «коммерческая тайна» получают сотрудники, включенные в список лиц, допущенных к конфиденциальной информации, который утверждается руководством правления АО «Узнацбанк». Указанный доступ формируется в соответствии с Матрицей доступа согласно приложению №10 к Политике информационной безопасности.

4.7 Запрещается распространение информационного актива с категорией конфиденциальная информация, третьим лицам.

5. Классификация информации и информационных ресурсов

5.1 Информация АО «Узнацбанк» классифицируется, чтобы определить требования к её защите, которые являются необходимым элементом организации работ по обеспечению информационной безопасности.

5.2 При классификации информации и информационных актов АО «Узнацбанк» должны учитываться:

- нормативно-методические основы для дифференцированного подхода к защите ресурсов информационной системы (информации, задач, рабочих мест, серверов, компьютеров) на основе их классификации по степени риска в случае нарушения их доступности, целостности или категорий доступа;
- требования законодательства;
- ценность и важность информационного ресурса для АО «Узнацбанк».

5.3 Классификация активов, её периодический пересмотр, а также обеспечение её актуальности и надлежащего уровня обеспечиваются владельцами информационного актива и УИБ ДИББ.

5.4 Уровень защиты можно оценить с помощью анализа конфиденциальности, целостности, доступности и других требований к информации.

Исходя из необходимости обеспечения различных уровней защиты разных видов информации, хранимой и обрабатываемой в АО «Узнацбанк», а также с учетом возможных путей нанесения ущерба АО «Узнацбанк» другим организациям или персоналу, вводятся категории доступа, целостности и доступности защищаемых информационных ресурсов.

5.5 Согласно установленному классу информации, должен организовываться соответствующий уровень доступа и защиты информационного актива.

6. Основные принципы классификации информации и информационных ресурсов

6.1 Информационные ресурсы АО «Узнацбанк» по категориям доступа разделяются на:

1) общедоступные информационные ресурсы (О) - предназначенные для неограниченного круга пользователей;

2) информационные ресурсы с ограниченным доступом (ДСП) - содержащие конфиденциальную информацию и предназначенную для ограниченного круга пользователей;

3) информационные ресурсы, составляющие коммерческую тайну (КТ).

6.2 К конфиденциальной информации относятся несекретные сведения ограниченного распространения, предусмотренные Перечнем сведений, отнесенных к конфиденциальной информации, согласно приложению № 2 к постановлению Кабинета Министров Республики Узбекистан от 7 ноября 2011 года № 296 «О мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572», а также указанные в Перечне защищаемой конфиденциальной информации АО «Узнацбанк», который определен в приложении №1 к Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

6.3 Информационные ресурсы АО «Узнацбанк» разделяются на следующие категории доступа:

1) беспрепятственная доступность (Б) - доступ к информационному ресурсу должен обеспечиваться в любое время (задержка не должна превышать нескольких секунд или минут);

2) высокая доступность (В) - доступ к информационному ресурсу должен осуществляться без существенных временных задержек (задержка не должна превышать нескольких часов);

3) средняя доступность (С) - доступ к информационному ресурсу может обеспечиваться с существенными временными задержками (задержка не должна превышать нескольких дней);

4) низкая доступность (Н) - временные задержки при доступе к информационному ресурсу практически не лимитированы (допустимая задержка получения результата - несколько недель).

6.4 Информационные ресурсы АО «Узнацбанк» разделяются на следующие категории целостности защищаемой информации:

1) высокая (В) - информационный ресурс, несанкционированная модификация или фальсификация которого может привести к нанесению значительного прямого ущерба, целостность которого должна обеспечиваться гарантированными методами (например, средствами электронной цифровой подписи) в соответствии с обязательными требованиями законодательства;

2) низкая (Н) - информационный ресурс, несанкционированная модификация или фальсификация которого может привести к нанесению незначительного косвенного ущерба, целостность которого должна обеспечиваться методами подсчета контрольных сумм, хеш-функций и т.п.;

3) нет требований (-) - информационный ресурс, к обеспечению целостности которого требования не предъявляются.

7. Порядок инвентаризации защищаемой информации

7.1 В целях определения информационных активов, ведения реестра и классификации информационных активов УИБ ДИББ ежегодно проводится инвентаризация имеющихся в АО «Узнацбанк» и его подразделениях информационных ресурсов.

7.2 В ходе инвентаризации информационных активов также определяется правильность их классификации в соответствии с настоящим Порядком, а также выполнение требований по их защите в соответствии с определенным для информационных активов класса защищенности.

7.3 По результатам инвентаризации могут вносится изменения и дополнения в Реестр, а также Перечень защищаемой конфиденциальной информации АО «Узнацбанк».

Также по итогам инвентаризации УИБ ДИББ выдает владельцам информационных активов предписание по устранению выявленных недостатков.

8. Маркировка активов

8.1 К информационным ресурсам АО «Узнацбанк» применяется процедура для маркировки информации при её обработке, в соответствии с системой классификации, принятой АО «Узнацбанк».

Процедуры маркировки относятся к информационным активам, представленным как в физической, так и в электронной форме.

8.2 Маркировка информационных активов осуществляется их владельцем.

8.3 Обычной формой маркировки являются физические метки. Информационные активы, как электронные документы, нельзя маркировать физически, поэтому необходимо использовать электронные средства маркировки, например, уведомляющие метки, которые могут появляться на экранах или дисплеях.

8.4 На метке или электронных средствах маркировки указывается порядковый номер информационного актива, гриф конфиденциальности, а также иная информация на усмотрении владельца информационного актива.

8.5 Маркировке подлежат напечатанные отчеты, экранные формы, носители информации (ленты, диски, компакт-диски, кассеты), электронные сообщения и передаваемые файлы.

8.6 В случае нецелесообразности использования маркировки, могут быть применены другие средства назначения уровня классификации информации.

8.7 Для каждого уровня классификации информационного актива его владельцем определяется порядок обработки и пользования информационным активом, включая безопасную обработку, хранение, передачу и уничтожение.

Данный порядок должен выполняться пользователями информационного актива.

8.8 Порядок обработки и пользования информационным активом также должен включаться в соглашения с другими организациями, предусматривающие совместное использование информации. Безопасное обращение с классифицированной информацией являются основным требованием к соглашениям по совместному использованию информации.

Приложение
к Порядку управления
информационными активами

Реестр информационных ресурсов АО «Узнацбанк»

№	Название ресурса	Описание ресурса	Размещение	Формат	Уровень конф-сти[1]	Целостность[2]	Доступность[3]	Частота обновления данных	Пользователи ресурсов[4]	Владелец[5]
1.	База данных ИАБС (копии и электронный архив)	Интегрированная автоматизированная банковская система АО «Узнацбанк»	Сервера БД и СХД основного и резервного ЦОД АО «Узнацбанк»	Цифровой	КТ	В	Б	Постоянное поступление данных	Сотрудники банка	ДИТ
2.	База данных БИС (копии и электронный архив)	Банковская информационная система АО «Узнацбанк»	Сервер БД и СХД в основном ЦОД АО «Узнацбанк»	Цифровой	КТ	В	В	Постоянное поступление данных с ИАБС	Сотрудники банка	ДИТ
3.	База данных системы ЭДО	Система электронного документооборота АО «Узнацбанк»	Сервер БД в основном ЦОД АО «Узнацбанк»	Цифровой	ДСП	В	В	Внос информации по мере необходимости	Сотрудники банка	ДИТ
4.	База данных процессинговой системы SWIFT	Система подключения АО «Узнацбанк» к международной системе SWIFT	Сервера БД в основном и резервном ЦОД АО «Узнацбанк»	Цифровой	КТ	В	Б	Поступление данных с ИАБС	Сотрудники банка	ДИТ

5.	База данных процессинговой системы VISA/ MasterCard	Система подключения АО «Узнацбанк» к международной системе VISA/MasterCard	Сервер БД в резервном ЦОД АО «Узнацбанк»	Цифровой	КТ	В	Б	Поступление данных с ИАБС	Сотрудники банка	ДРБ
6.	База данных Центра регистрации ключей ЭЦП	Сертификаты открытых ключей ЭЦП сотрудников и клиентов банка	Сервер ЦРК ЭЦП в основном ЦОД АО «Узнацбанк»	Цифровой	ДСП	В	Б	Внос информации по мере необходимости	Администратор ЦРК ЭЦП	ДИББ
7.	Файл сервер FTP	Хранилище файлов сотрудников банка головного офиса и областных филиалов	FTP-сервера в головном офисе и областных филиалах	Цифровой	ДСП	Н	С	Внос информации по мере необходимости	Сотрудники банка	ДИТ, Сектора автоматизации областных филиалов
8.	Официальный веб-сайт nbu.uz	Официальный веб-сайт АО «Узнацбанк»	Хостинг в ЦОД AB Digital	Цифровой	О	Н	В	При необходимости обновления информации на сайте	Сотрудники банка, пользователи Интернет	Департамент развития сети и сервиса банка
9.	Веб-сайты Интернет-банкинга(milliy.nbu.uz и ibank.nbu.uz/)	Оказание услуг клиентам банка через Интернет	Сервера приложений в основном ЦОД АО «Узнацбанк»	Цифровой	О	В	В	При необходимости обновления информации на сайте	Интернет клиенты банка	ДИТ
10.	Документированная информация «ДСП»	Конфиденциальная информация с грифом «ДСП»	Сейфы подразделений управления делами головного офиса, областных и районных филиалов	Бумажный	ДСП	В	С	По мере необходимости	Сотрудники банка	Управление делами головного офиса, областных и районных филиалов
11.	Данные сотрудников банка	Персональная информация о сотрудниках банка	Рабочие станции, сейфы и шкафы подразделений по работе с персоналом	Бумажный и цифровой	ДСП	В	С	По мере необходимости	Сотрудники банка	Подразделения по работе с персоналом головного офиса,

			головного офиса, областных и районных филиалов							областных и районных филиалов
12	Финансовые данные	Коммерческая информация	Рабочие станции, сейфы и шкафы подразделений бухгалтерского учета и отчетности головного офиса, областных и районных филиалов	Бумажный и цифровой	КТ	В	С	По мере необходимости	Сотрудники банка	Подразделения бухгалтерского учета и отчетности головного офиса, областных и районных филиалов

[1]Уровень конфиденциальности: ДСП – ограниченного доступа, КТ– коммерческая тайна и О - открытая;

[2]Целостность: В, Н – (нет требований);

[3]Доступность: Б, В, С, Н;

[4]Пользователи: подразделение АО «Узнацбанк», которому санкционирована работа с ресурсом на основе матрицы доступа;

[5]Владелец: Подразделение, ответственное за формирование, ведение и обслуживание информационного ресурса.

Приложение №14
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 27.12.2021г

Инструкция по организации технической защиты информации

1. Общие положения

1.1 Настоящая Инструкция определяет основные меры, методы и средства технической защиты информации, входящих в систему защиты информации АО «Узнацбанк» и порядок их реализации.

1.2 Требования настоящей Инструкции являются обязательными для применения в АО «Узнацбанк».

1.3 Обеспечение технической защиты информации является обязанностью УИБ ДИББ, Отделов по безопасности, режиму и защите информации областных филиалов и главных специалистов по безопасности, режиму и защите информации районных филиалов (далее – подразделения информационной безопасности).

1.4 УИБ ДИББ совместно с подразделениями ДИТ и ДРБ обеспечивает реализацию мер и контролирует выполнение установленных требований по организации технической защиты информации в АО «Узнацбанк».

2. Основные понятия и сокращения

2.1 В настоящей Инструкции применены следующие термины и определения:

средства технической защиты информации - аппаратные, программные или аппаратно-программные средства, осуществляющие защиту информации и обеспечивающие безопасность информации на всех стадиях ее жизненного цикла (формирования, передачи, приема, преобразования, отображения и хранения информации).

техническая защита информации: деятельность, направленная на обеспечение безопасности информации, инженерно-техническими и не криптографическими методами с использованием средств технической защиты информации.

2.2 В настоящей Инструкции используются следующее сокращения:

IDPS (Intrusion Detection & Prevention System) – средства (система) обнаружения и предотвращения вторжений;

DLP (Data Loss Prevention) – система предотвращения утечек конфиденциальной информации;

SIEM (Security Information and Event Management) – система управления инцидентами информационной безопасности.

3. Порядок организации технической защиты информации

3.1 Организацию технической защиты информации в АО «Узнацбанк» обеспечивает УИБ ДИББ. С этой целью данным управлением:

- разрабатываются требования к обеспечению технической защиты информации и организации системы защиты информации в АО «Узнацбанк»;
- подготавливаются планы по развитию системы защиты информации и внедрению средств технической защиты информации;
- вырабатываются требования к средствам технической защиты информации, организуется их закупка, внедрение и ввод в эксплуатацию;
- осуществляется эксплуатация системы защиты информации и входящих в неё средств технической защиты информации.

3.2 Организация технической защиты конфиденциальной информации должна обеспечиваться с выполнением требований постановления Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

3.3 Согласно постановлению Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 УИБ ДИББ создает (модернизирует) систему защиты информации по следующим этапам:

- предпроектное обследование, разработка обоснования необходимости создания (модернизации) системы защиты;
- проектирование (разработка проектов) и реализация системы защиты информатизации.
- ввод в действие системы защиты информации, с проведением опытно-эксплуатационных и приемо-сдаточных испытаний средств защиты.

По результатам предпроектного обследования разрабатывается техническое задание на разработку системы защиты информации.

На стадии проектирования и реализации системы защиты осуществляется разработка технического проекта, разработка организационно-технических мероприятий, закупка средств защиты информации и их установка, при необходимости разработка программных средств защиты информации.

На стадии ввода в действие системы защиты информации осуществляется опытная эксплуатация, отработка технологических процессов защиты информации, приемо-сдаточные испытания.

3.4 Указанные в настоящей Инструкции меры и средства технической защиты информации реализуются подразделениями информационной безопасности.

Для их реализации подготавливаются ежегодные планы мероприятий по обеспечению информационной безопасности, включающие мероприятий по приобретению, установке, настройке, испытанию и вводу эксплуатацию средств технической защиты информации.

4. Основные направления и методы технической защиты информации

4.1 Технические меры защиты информации должны реализовываться по следующим основным направлениям:

- сетевая безопасность;
- защита информации от вредоносных программ;
- защита от несанкционированного доступа;
- защита информации от утечки по техническим каналам;
- контроль и анализ обеспечения информационной безопасности.

4.2 Технической защите подлежат все компоненты банковской информационной инфраструктуры АО «Узнацбанк», информационные системы и ресурсы АО «Узнацбанк».

4.3 Технические методы защиты информации должны реализовываться при создании системы защиты информации в АО «Узнацбанк».

5. Используемые методы и средства технической защиты информации

5.1 Сетевая безопасность

5.1.1 К средствам технической защиты информации, обеспечивающих сетевую безопасность в АО «Узнацбанк» относятся межсетевые экраны, прокси-сервера, средства IDPS.

5.1.2 В АО «Узнацбанк» должны быть предусмотрены меры межсетевого экранирования и применения межсетевых экранов в соответствии с Положением по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, приведенным в приложении №2 к Политике информационной безопасности АО «Узнацбанк».

5.1.3 Защита от сетевых вторжений и атак должна обеспечиваться с применением средств IDPS на границе подключения корпоративной сети АО «Узнацбанк» к внешней сети (Интернет, TAS-IX и МСПД). Применение средств IDPS должно обеспечиваться на всех организуемых точках подключения корпоративной сети к внешней сети, а также основного и резервного ЦОД к корпоративной сети.

5.1.4 В АО «Узнацбанк» используются следующие межсетевые экраны и средства IDPS:

1) Аппаратно-программный межсетевой экран CheckPoint 4800 шлюз безопасности с функциями IDPS на границе подключения корпоративной сети к сети Интернет (TAS-IX) и МСПД.

Объект защиты: корпоративная сеть, ЛВС головного офиса и основной ЦОД.

Место размещение: коммутационное помещение головного офиса.

2) Аппаратно-программный межсетевой экран нового поколения Cisco FirePower 4110 на границе подключения DMZ основного ЦОД к ЛВС головного офиса и корпоративной сети.

Объект защиты: DMZ основного ЦОД.

Место размещение: серверное помещение основного ЦОД.

3) Аппаратно-программный межсетевой экран нового поколения Cisco FirePower 2120 на границе подключения DMZ резервного ЦОД к корпоративной сети.

Объект защиты: DMZ резервного ЦОД.

Место размещение: серверное помещение резервного ЦОД.

4) Аппаратно-программный межсетевой экран CheckPoint 4800 шлюз безопасности с функциями IDPS на границе подключения резервного ЦОД (системы процессинга VISA/MasterCard АО «Узнацбанк») к внешней сети.

Объект защиты: ЛВС резервного ЦОД и системы процессинга VISA/MasterCard АО «Узнацбанк».

Место размещение: серверное помещение резервного ЦОД.

Указанные выше межсетевые экраны подлежат резервированию.

5.1.5 Для управления доступом к сети Интернет сотрудников АО «Узнацбанк», информационных систем и ресурсов на границе подключения корпоративной сети к внешней сети используется единый прокси-сервер, реализованный на базе аппаратно-программного Интернет-шлюза «Интернет Контроль Сервер».

Объект защиты: корпоративная сеть, ЛВС головного офиса.

Место размещение: коммутационное помещение головного офиса.

5.1.6 В целях фильтрации нежелательного сетевого трафика в настройках средств IDPS, прокси-сервера и межсетевых экранов должны использоваться функции URL-фильтр, спам-фильтр, фильтр прикладного уровня и контроль трафика на наличие вредоносных программ.

5.1.7 При организации связи должны выполняться следующие требования:

- подключение сотрудников банка и банкоматов к ИАБС и другим информационным системам АО «Узнацбанк» должно осуществляться через корпоративную сеть;
- запрещено предоставлять доступ к сети Интернет (TAS-IX) рабочим станциям, серверам, банкоматам, подключенные или используемым в ИАБС.

5.2 Защита от вредоносных программ

5.2.1 В АО «Узнацбанк» должны предусматриваться следующие технические меры защиты от вредоносных программ, включая компьютерные вирусы, черви, троянские и шпионские программы, эксплойты и др:

- применение средств защиты от вредоносных программ (антивирусы);
- настройка веб-браузеров для повышения уровня безопасности, включая блокировку появляющихся окон и веб-рекламы, предупреждения при попытке загрузить вредоносный или подозрительный контент, использование безопасного режима просмотра веб-сайтов и др.
- постоянная проверка средствами антивирусной защиты съемных носителей на наличие вредоносных программ перед их применением в средствах обработки, хранения и передачи информации;
- проверка средствами антивирусной защиты любой электронной информации, полученной банком по сети Интернет и электронной почте;
- ограничение использования на серверах и рабочих станциях съемных носителей;

- блокировка доступа к вредоносным сайтам средствами контентной фильтрации трафика и с помощью прокси-сервера;

- запрещение установки сотрудниками банка неразрешенных программ на рабочих станциях;

- применение мер по ограничению использования пользователями анонимайзеров и TOR-сетей.

5.2.2 Антивирусная защита должна обеспечиваться применением антивирусных средств защиты от вредоносных программ, устанавливаемых на рабочих станциях и серверах.

Антивирусная защита должна организовываться и обеспечиваться в соответствии с Инструкцией по антивирусной защите, приведенной в приложении №8 к Политике информационной безопасности АО «Узнацбанк».

5.2.3 В АО «Узнацбанк» применяются системы централизованного управления антивирусными программами, установленными на рабочих станциях и серверах (далее – централизованная антивирусная система):

- централизованная антивирусная система в г. Ташкенте, охватывающая все рабочие станции и сервера головного офиса и Главного управления по Ташкенту и его структурных подразделений в г. Ташкенте, включая минибанки;

- централизованная антивирусная система, установленная в каждом областном филиале и охватывающая все рабочие станции и сервера областного филиала и подчиненных ему районных филиалов и минибанков.

В качестве централизованной антивирусной системы используется ESET Protect.

5.2.4 В целях фильтрации нежелательного сетевого трафика в настройках средств IDPS, прокси-сервера и межсетевых экранов должны использоваться функции URL-фильтр, спам-фильтр и контроль трафика на наличие вредоносных программ.

5.3 Защита от несанкционированного доступа

5.3.1 В АО «Узнацбанк» должны предусматриваться следующие технические методы защиты от несанкционированного доступа:

- использование инженерных средств защиты (двери, стены, потолки, решетки на окнах, заборы, ограждения и т.д.), оборудованные замками (механическими, электромеханическими, электрическими), пломбами, препятствующих или преграждающих несанкционированные физические проникновения;

- применение на внешнем корпусе средств обработки, хранения и передачи информации замков, в том числе одноразовых, пломб, защитных липких лент или защитных и голографических этикеток;

- установка системы охранной сигнализации и системы видеонаблюдения в защищаемых помещениях;

- применение средств контроля доступа и аутентификации при доступе в помещения (СКУД, кодовые замки, идентификационные магнитные карты), к средствам обработки, хранения и передачи информации, сети, информационным ресурсам и системам.

5.3.2 Для контроля, разграничения и управления доступом к сетевым

ресурсам (сетевые файловые хранилища данных, принтеры, рабочие станции и др.), службам (электронная почта и др.), ведения учетной записи пользователей и рабочих станций в ЛВС головного офиса, областных и районных филиалов должна применяться служба каталогов (Directory Service и др.).

5.3.2 Система контроля, разграничения и управления доступом к сетевым ресурсам и информационным системам должна организовываться в соответствии с требованиями Инструкции по парольной защите и аутентификации, приведенной в приложении №7 к Политике информационной безопасности АО «Узнацбанк».

5.4 Защита информации от утечки по техническим каналам

5.4.1 Основными методами защиты информации от утечки по техническим каналам являются:

- использование сертифицированных по требованиям защиты информации основных технических средств и систем, предназначенных для передачи, обработки и хранения информации;
- размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от её границ;
- документальное оформление перечня защищаемых помещений и лиц, ответственных за их эксплуатацию;
- выполнение рекомендованных мероприятий по оборудованию защищенных помещений: стены, полы и потолки не должны быть смежными с помещениями других организаций, окна закрываются шторами (жалюзи);
- проведение специальных проверок помещений для выявления технических каналов утечек информации, включая несанкционированное подключение к каналам, сети, средствам обработки, хранения и передачи информации.

5.4.2 В целях защиты конфиденциальной информации от утечек из банковской информационной системы АО «Узнацбанк» должно предусматриваться применение систем предотвращения утечек конфиденциальной информации (DLP).

Система DLP должна контролировать все возможные каналы утечек конфиденциальной информации, вести учет конфиденциальной информации в банковской информационной системы и действий над ней, выявлять и сообщать факты утечек, обнаруживать нарушителей, осуществлять сбор и хранение неопровержимых свидетельств о совершении нарушений.

5.5 Контроль и анализ обеспечения информационной безопасности

5.5.1 Для обеспечения анализа и контроля защищенности в АО «Узнацбанк» применяются средства мониторинга и средства контроля эффективности защиты информации.

5.5.2 Для мониторинга состояния функционирования корпоративной сети, основных серверов и сетевого оборудования в головном офисе в ДИТ создан и функционирует Центр мониторинга, который работает круглосуточно. Данный центр организован на базе программного обеспечения Zobbix.

5.5.4 Для выявления (мониторинга) и управления инцидентами информационной безопасности в АО «Узнацбанк» применяется система SIEM – IBM QRadar SIEM.

Указанная система позволяет быстро распознавать и определять эскалацию известных угроз безопасности, быстро и эффективно реагировать на них, использоваться для эффективной работы операционного центра безопасности (SOC).

5.5.5 В целях анализа и контроля защищенности в АО «Узнацбанк» используется система MaxPatrol 8.

MaxPatrol 8 является программным комплексом, который обеспечивает контроль защищенности и соответствия стандартам безопасности информационных систем АО «Узнацбанк» с применение механизмов тестирования на проникновение, системных проверок и контроля соответствия стандартам. Система позволяет получать объективную оценку состояния защищенности IT-инфраструктуры в целом, а также отдельных подразделений, узлов и приложений, что необходимо для своевременного обнаружения уязвимостей и предотвращения атак с их использованием.

5.5.6 По результатам анализа защищенности должны приниматься соответствующие меры по повышению уровня обеспечения информационной безопасности и устранению выявленных недостатков в системе защиты информации АО «Узнацбанк».

6. Применение мер и средств технической защиты информации

6.1 Эксплуатация средств технической защиты информации осуществляется сотрудниками подразделений информационной безопасности в соответствии с требованиями Политики информационной безопасности АО «Узнацбанк», а также согласно Инструкциям и руководствам по эксплуатации технических и программных средств защиты информации.

6.2 Инструкции и руководства по эксплуатации технических и программных средств защиты информации разрабатываются УИБ ДИББ в отношении каждого средства технической защиты внедряемого и используемого в АО «Узнацбанк». Указанные инструкции разрабатываются на основе руководств и эксплуатационных документов разработчиков или производителей этих средств.

7. Ответственность

7.1 Подразделения информационной безопасности несут ответственность за реализацию мер технической защиты информации в соответствии с настоящей Инструкцией.

7.2 Нарушение требований, установленных настоящей Инструкцией, влечёт за собой наложение дисциплинарной ответственности в соответствии с внутренним трудовым распорядком и трудовым законодательством Республики Узбекистан.

Приложение №15
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 от 27.12.2024г

Инструкция по организации криптографической защиты информации

1. Общие положения

1.1 Настоящая Инструкция определяет основные меры, методы и средства криптографической защиты информации, входящих в систему защиты информации АО «Узнацбанк» и порядок их реализации, а также регламентирует действия сотрудников банка, допущенных к работе со средствами криптографической защиты информации (СКЗИ) и криптографическими ключами шифрования и ЭЦП.

1.2 Требования настоящей Инструкции являются обязательными для применения в АО «Узнацбанк» и исполнения его сотрудниками.

1.3 Криптографическая защита информации в АО «Узнацбанк» используется для:

- организации защищенной передачи информации по корпоративной сети АО «Узнацбанк» при работе сотрудников банка с ИАБС, а также по внешней сети клиентами банка при пользовании Интернет-банкингом и мобильным банкингом;
- формирования и проверки ЭЦП для обеспечения авторства и целостности информации при обмене информацией с информационными системами АО «Узнацбанк»;
- аутентификации сотрудников банка и клиентов Интернет-банкиннга и мобильного банкинга при доступе к ИАБС.
- для защищенного обмена информацией с применением систем E-xat и E-ijro, в которых обеспечивается шифрование передаваемой информации, формирование и проверка ЭЦП.

1.4 Обеспечение криптографической защиты информации является обязанностью УИБ ДИББ, Отделов по безопасности, режиму и защите информации областных филиалов.

1.5 УИБ ДИББ совместно с подразделениями ДИТ и ДРБ обеспечивает реализацию мер и контролирует выполнение установленных требований по организации криптографической защиты информации в АО «Узнацбанк».

1.6 Применяемые в АО «Узнацбанк» СКЗИ должны быть сертифицированы в соответствие постановлением Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан».

2. Основные понятия и сокращения

2.1 В настоящей Инструкции применены следующие термины и определения:

криптографический алгоритм (криптоалгоритм) — математический алгоритм преобразования информации (данных) с целью предотвращения возможности ее искажения и защиты от несанкционированного доступа;

криптографическая защита информации — комплекс мероприятий, направленных на обеспечение целостности, доступности и конфиденциальности информации, осуществляемых при помощи алгоритмов криптографического преобразования (криптоалгоритмов);

криптографический ключ - последовательность секретных символов, которые выполняют шифрование, дешифрование, формирование и проверку электронных подписей с использованием криптографических алгоритмов;

криптографическая система (криптосистема) — совокупность организационных, технических и программных средств, обеспечивающих криптографическое преобразование информации и (или) управление, в том числе автоматизированное, процессом изготовления и распределения криптографических ключей;

средства криптографической защиты информации (СКЗИ) — аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности, в том числе:

а) средства шифрования — аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи;

б) средства имитозащиты — аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи — совокупность технических и программных средств, обеспечивающих создание электронной цифровой подписи в электронном документе, подтверждение подлинности электронной цифровой подписи, создание открытых и закрытых ключей электронной цифровой подписи;

г) средства кодирования — средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций;

д) средства изготовления ключевых документов и сами ключевые документы (независимо от вида носителя ключевой информации);

шифрование: совокупность обратимых преобразований информации (данных) в соответствии с криптографическим алгоритмом и ключом для надежного сокрытия ее истинного содержания.

2.2 В настоящей Инструкции используются следующие сокращения:

СКЗИ – средства криптографической защиты информации;

ЭЦП – электронная цифровая подпись.

3. Порядок организации криптографической защиты информации

3.1 Организацию криптографической защиты информации в АО «Узнацбанк» обеспечивает УИБ ДИББ. С этой целью данным управлением:

- разрабатываются требования к обеспечению криптографической защиты информации и применению СКЗИ в АО «Узнацбанк»;
- подготавливаются планы по развитию криптографической системы и внедрению СКЗИ;
- вырабатываются требования к СКЗИ, организуется их закупка, внедрение и ввод в эксплуатацию и сертификацию;
- осуществляется эксплуатация криптографической системы и входящих в неё СКЗИ.

3.2 Указанные в настоящей Инструкции меры и средства криптографической защиты информации реализуются подразделениями информационной безопасности.

Для их реализации подготавливаются ежегодные планы мероприятий по обеспечению информационной безопасности, включающие мероприятий по внедрению и применению СКЗИ.

3.3 Эксплуатация СКЗИ осуществляется сотрудниками банка в соответствии с инструкциями по их эксплуатации от разработчиков (производителей) этих СКЗИ.

3.4 Инструкции по эксплуатации СКЗИ доводятся до сотрудников АО «Узнацбанк» УИБ ДИББ.

4. Используемые методы и средства криптографической защиты информации

4.1 В АО «Узнацбанк» СКЗИ применяются:

1) сотрудниками банка в ИАБС для обеспечения шифрования данных, формирования и проверки ЭЦП (для аутентификации пользователей и целостности передаваемых данных) при обмене информацией с базой данных ИАБС;

2) клиентами банка при пользовании Интернет-банкингом и мобильным банкингом для шифрования данных, формирования и проверки ЭЦП (для аутентификации пользователей и целостности передаваемых данных) при обмене информации с сервером приложений ИАБС;

3) сотрудники банка (операторы денежных переводов) и администратор систем при работе в международных системах денежных переводов для шифрования данных, формирования и проверки ЭЦП (для аутентификации пользователей и целостности передаваемых данных) при обмене информацией в международной системе денежных переводов;

4) отдельные сотрудники банка в системе защищенной электронной почты E-xat и системе контроля исполнительской дисциплины E-ijro для обеспечения защищенной передачи информации по системам (шифрование данных, формирование и проверка ЭЦП) между головным офисом, областными и районными филиалами, а также сторонними организациями.

4.2 В ИАБС применяется программное СКЗИ, обеспечивающее формирование и проверку ЭЦП (средство ЭЦП) в соответствии со стандартом O'zDSt 1092-2009 и криптографическое шифрование передаваемой информации (средство шифрование) в соответствии со стандартом O'zDSt 1105-2009.

СКЗИ устанавливается на рабочих станциях сотрудников банка, являющихся авторизованными пользователями ИАБС.

4.3 Все ответственные сотрудники банка, вводящие, утверждающие и производящие соответствующие операции с электронными платёжными документами в системе ИАБС, должны быть обеспечены криптографическими закрытыми ключами (закрытый ключ ЭЦП и шифрования), используемыми в ИАБС.

4.4 При пользовании клиентами банка Интернет-банкингом и мобильным банкингом АО «Узнацбанк» ими используются программные СКЗИ, обеспечивающее формирование и проверку ЭЦП (средство ЭЦП) в соответствии со стандартом O'zDSt 1092-2009 и криптографическое шифрование передаваемой информации (средство шифрование) в соответствии со стандартом O'zDSt 1105-2009. Указанные программные СКЗИ устанавливаются на рабочих станциях и мобильных устройствах клиентов банка.

4.5 Криптографические ключи шифрования и ЭЦП генерируются и выдаются сотрудникам банка, являющиеся авторизованными пользователями ИАБС, а также авторизованным клиентам Интернет-банкинга и мобильного банкинга УИБ ДИББ с применением программного обеспечения Центра регистрации ключей ЭЦП.

Процесс генерирования криптографических ключей шифрования и ЭЦП должен быть защищен.

4.6 Созданные криптографические ключи шифрования и ЭЦП для сотрудников банка (пользователей ИАБС) записываются на защищенный USB-носитель (token).

4.7 Криптографические ключи шифрования и ЭЦП автоматизированных клиентов банка должны регистрироваться на защищенных USB-носителях (E-Pass), выдаваемых клиентам банка или мобильных устройствах и защищаться от несанкционированного копирования любым способом.

4.8 Порядок выдачи криптографических ключей шифрования и ЭЦП, их плановая и внеплановая смена определены в Инструкции по парольной защите и аутентификации, приведенной в приложении №7 к Политике информационной безопасности АО «Узнацбанк».

4.9 Для проверки ЭЦП сотрудников и клиентов банка Центром регистрации ключей ЭЦП АО «Узнацбанк» изготавливаются сертификаты открытых ключей ЭЦП, которые заносятся в базу Центра регистрации.

4.10 Обеспечение функционирования Центра регистрации ключей ЭЦП, его администрирование, изготовление криптографических закрытых и открытых ключей ЭЦП осуществляется УИБ ДИББ в соответствии с Положением о порядке работы Центра регистрации ЭЦП АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан»

4.11 Срок действия сертификата ключа ЭЦП, изготовленных Центром регистрации ключей ЭЦП АО «Узнацбанк», не должен превышать 24 месяца с

даты регистрации ЭЦП.

Смена криптографических закрытых ключей должна производиться по истечение срока действия сертификата открытого ключа ЭЦП.

4.12 Криптографические ключи шифрования и ЭЦП применяются сотрудниками банка (операторы денежных переводов) и администратором систем при работе в международных системах денежных переводов.

Криптографические ключи шифрования и ЭЦП формируются и выдаются операторами международных систем денежных переводов.

4.13 Также СКЗИ применяются в системе защищенной электронной почты E-xat и системе контроля исполнительской дисциплины E-ijro для обеспечения защищенной передачи информации по системам.

Пользователи систем E-xat и E-ijro среди сотрудников АО «Узнацбанк» определяются его руководством.

Пользователям систем E-xat и E-ijro выдаются криптографические ключи шифрования и ЭЦП, а также сертификаты открытых ключей ЭЦП, которые обеспечивают аутентификацию пользователей на основе их ЭЦП в системах, шифрование вводимой и передаваемой информации, а также формирование ЭЦП в вводимой информации для обеспечения её целостности при передаче.

Криптографические ключи шифрования и ЭЦП, а также сертификаты открытых ключей ЭЦП генерируются и выдаются на защищенном USB-носителе пользователям систем E-xat и E-ijro, являющиеся сотрудниками АО «Узнацбанк».

Генерацию криптографических ключей шифрования и ЭЦП и формирование сертификатов открытых ключей производит зарегистрированный в установленном порядке Центр регистрации ключей ЭЦП ГУП «UNICON.UZ» на основании договоров, заключенных между ГУП «UNICON.UZ» и АО «Узнацбанк» на оказание услуг E-xat и E-ijro.

В системах E-xat и E-ijro применяются программные СКЗИ ГУП «UNICON.UZ», обеспечивающие формирование и проверку ЭЦП (средство ЭЦП) в соответствии со стандартом O'zDSt 1092-2009 и криптографическое шифрование передаваемой информации (средство шифрование) в соответствии со стандартом O'zDSt 1105-2009. СКЗИ установлено на защищенном USB-носителе, которое обеспечивается формирование и проверку ЭЦП, а также шифрование при его подключении к рабочей станции пользователей систем.

Установку и настройку на рабочих станциях сотрудников банка СКЗИ и клиентских программ систем E-xat и E-ijro осуществляется подразделениями информационной безопасности.

4.14 Применяемые в АО «Узнацбанк» СКЗИ должны быть сертифицированы в установленном порядке.

4.15 Криптографические закрытые ключи ЭЦП и шифрования должны использоваться только их владельцами.

5. Обязанности и ответственность сотрудников при пользовании СКЗИ

5.1 Сотрудники банка, работающие с криптографическими ключами, обязаны:

- обеспечивать сохранность криптографических ключей и в случае их неиспользования хранить защищенных местах (сейфах);
- не передавать криптографические ключи, а также не сообщать пароли доступа к криптографическому ключу другим сотрудникам банка и посторонним лицам;
- при неиспользовании криптографических ключей (завершение рабочего дня, выход в отпуск или на больничный и т.д.) сдать его начальнику своего подразделения или в подразделение информационной безопасности. Неиспользуемые криптографические ключи сотрудников банка должны храниться в сейфах;
- не оставлять носитель криптографических ключей на рабочем месте без присмотра в момент отсутствия сотрудника или при не работе в ИАБС;
- немедленно сообщать администратору информационной безопасности в случаях: утери и хищения криптографического ключа, компрометации криптографического ключа, повреждении носителя криптографического ключа, возникновения проблем при доступе в ИАБС;
- сдать носитель с криптографическим ключом при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- не использовать предоставленный защищенный носитель для иных целей, кроме как для хранения криптографических ключей.

5.2 Обязанности и ответственность клиентов банка по защите выданных им криптографических ключей оговариваются в договоре на оказание банковских услуг.

5.3 Вышедшие из строя криптографические ключи и/или их носители возвращаются в подразделение информационной безопасности для последующей замены в установленном порядке.

5.4 Подразделения информационной безопасности АО «Узнацбанк» обязаны обеспечивать учет выданных сотрудникам АО «Узнацбанк» криптографических ключей и их носителей в специальных журналах.

6. Ответственность

6.1 Подразделения информационной безопасности несут ответственность за реализацию мер криптографической защиты информации в соответствии с настоящей Инструкцией

6.2 Сотрудники банка, работающие с криптографическими ключами, несут персональную ответственность за нарушение настоящей Инструкции.

6.3 Подразделения информационной безопасности являются ответственными за обеспечение контроля выполнения настоящей Инструкции сотрудниками АО «Узнацбанк».

6.4 Нарушение требований, установленных настоящей Инструкцией, влечёт за собой наложение дисциплинарной ответственности в соответствии с внутренним трудовым распорядком и трудовым законодательством Республики Узбекистан.

Приложение №16
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-6 27.12.2021г

Порядок обращения с информацией, подлежащей защите

1. Общие положения

1.1 Настоящий Порядок определяет требования сотрудников головного офиса, областных и районных филиалов АО «Узнацбанк» по обращению с информацией, подлежащей защите.

1.2 Требования по обращению сотрудников АО «Узнацбанк» с информацией, подлежащей защите, определены внастоящем Порядке в соответствии с требованиями постановления Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295«Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан» и Инструкции о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения», утвержденной 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан - председателем межведомственной комиссии по вопросам защиты государственных секретов.

2. Информация, подлежащая к защите

2.1 К защите и не распространению подлежат:

- конфиденциальная информация, входящая в Перечень конфиденциальной информации АО «Узнацбанк», который определен в Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан»;
- конфиденциальная информация, содержащаяся в информационных ресурсах, входящих в Реестр информационных ресурсов АО «Узнацбанк» и имеющих уровень конфиденциальности – конфиденциальная в соответствии с Порядком управления информационными активами, приведенным в приложении №13 к Политике информационной безопасности АО «Узнацбанк»;
- документы, дела и издания, содержащие несекретные сведения ограниченного распространения.

2.2 К конфиденциальной информации относятся сведения, перечень которых определен в приложении № 2 к постановлению Кабинета Министров Республики Узбекистан от 7 ноября 2011 года № 296 «О мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572».

2.3 Перечень конфиденциальной информации АО «Узнацбанк», включая документированную информацию и информацию в электронном виде, должен формироваться в соответствии с постановлением Кабинета Министров

Республики Узбекистан от 16 октября 2015 года №295«Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

Перечень конфиденциальной информации АО «Узнацбанк» определен в Инструкции по обеспечению безопасности конфиденциальной информации на объектах информатизации акционерного общества «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

Пересмотр перечня конфиденциальной информации должен проводиться не реже одного раза в три года по результатам инвентаризации, который проводится УИБ ДИББ.

2.4 Контроль за формированием, ведением и доведением Перечня конфиденциальной информации АО «Узнацбанк» до его сотрудников осуществляет УИБ ДИББ, а в областных и районных филиалах – Отделы по безопасности, режиму и защите информации областных филиалов и главные специалисты по безопасности, режиму и защите информации районных филиалов.

2.5 Уровень конфиденциальности информационных ресурсов АО «Узнацбанк» определяется в соответствии с Порядком управления информационными активами, приведенным в приложении №13 к Политике информационной безопасности АО «Узнацбанк».

2.6. Документы, дела и издания, содержащие несекретные сведения ограниченного распространения определяются в соответствии Инструкцией о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения», утвержденной 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан - председателем межведомственной комиссии по вопросам защиты государственных секретов.

К указанным сведениям ограниченного распространения относятся несекретные сведения, предусмотренные Перечнем сведений, запрещенных к опубликованию, Агентства информации и массовых коммуникаций при Администрации Президента Республики Узбекистан, перечнями сведений АО «Узнацбанк» и иных министерств и ведомстве, не подлежащих обнародованию в открытой печати, передачах по радио и телевидению, и другие сведения, открытое опубликование которых может нанести вред Республике Узбекистан.

3. Требования по обращению с информацией, подлежащей защите

3.1 Информация, подлежащая к защите, указанная в пункте 2.1 настоящего Порядка, не подлежит:

- передаче и раскрытию третьим лицам, не являющимся сотрудниками АО «Узнацбанк»;
- распространению в сети Интернет, обнародованию в открытой печати, передачах по радио и телевидению и в других средствах массовой коммуникации;
- передаче по каналам связи вне контролируемой зоны или через корпоративную электронную почту без применения сертифицированных средств

криптографической защиты информации, если даже эта информация предназначена сотруднику АО «Узнацбанк».

3.2 Защита конфиденциальной информации АО «Узнацбанк», в том числе в информационных системах, осуществляется в соответствии с требованиями постановления Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295«Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

3.3 Запрещается доступ к конфиденциальной информации, входящий в Перечень конфиденциальной информации АО «Узнацбанк», лиц, не являющихся сотрудниками банка, а также сотрудникам банка, которым данная информация не принадлежит по роду своей деятельности.

Ответственность за выполнение данного требования лежит на сотрудников банка, обеспечивающих формирование, хранение и предоставление конфиденциальной информации, а также сотрудников банка, управляющих доступом к конфиденциальной информации.

3.4 Ответственность за защиту и нераспространение информации, содержащейся в информационных ресурсах с уровнем конфиденциальности – конфиденциальная, несут их владельцы и УИБ ДИББ. Контроль за обеспечением защиты и нераспространением информации, содержащейся в информационных ресурсах с уровнем конфиденциальности – конфиденциальная, обеспечивается УИБ ДИББ.

3.5 На документах, делах и изданиях, содержащих несекретные сведения ограниченного распространения, указанных в пункте 2.6 настоящего Порядка, проставляется гриф «ДСП», а на документах и изданиях, кроме того, - номер экземпляров.

3.6 Определение необходимости проставления грифа «ДСП» производится на основании перечней, указанных в пункте 2.6 настоящего Порядка: на документе – исполнителем и лицом, подписывающим документ, а на издании – автором (составителем) и руководителем, утверждающим издание к печати.

3.7 Учет, размножение, хранение, использование, отбор на хранение и уничтожение документов, дел и изданий, содержащих несекретные сведения ограниченного распространения, должен производиться сотрудниками банка в соответствии с Инструкцией о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения», утвержденной 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан - председателем межведомственной комиссии по вопросам защиты государственных секретов.

3.8 Сотрудники банка, имеющие отношение к работе с документами, делами и изданиями с грифом «ДСП», должны быть в обязательном порядке ознакомлены с настоящим Порядком и Инструкцией о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения», утвержденной 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан - председателем межведомственной комиссии по вопросам защиты государственных секретов.

3.9 Руководители структурных подразделений АО «Узнацбанк» и соответствующие должностные лица несут ответственность за обеспечение правильного ведения учета, хранения, размножения и использования документов, дел и изданий с грифом «ДСП», а также за соблюдение требований настоящего Порядка и Инструкции о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения», утвержденной 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан - председателем межведомственной комиссии по вопросам защиты государственных секретов.

3.10 Контроль за осуществлением учета, размножения, хранения и использования документов, дел и изданий с грифом «ДСП», а также за неразглашение сведений, содержащихся в документах, делах и изданиях с грифом «ДСП» возлагается на подразделения по управлению делами головного офиса, областных и районных филиалов.

4. Ответственность

4.1 Ответственность за соблюдение требований настоящего Порядка возлагается на руководителей структурных подразделений, сотрудников банка и соответствующих должностных лиц АО «Узнацбанк».

Приложение №17
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-1 27.12.2021г

План обеспечения непрерывной работы и восстановления работоспособности в чрезвычайных (аварийных) ситуациях

1. Общие положения

1.1 Настоящий План предназначен для обеспечения непрерывной работы и восстановления работоспособности технических средств обработки, передачи, хранения информации и средств защиты информации, используемых в ЦОД, головном офисе, областных и районных филиалах, минибанках АО «Узнацбанк».

1.2 К мерам обеспечения непрерывной работы информационных ресурсов и систем АО «Узнацбанк» относятся:

- плановые профилактические и ремонтные работы;
- резервирование аппаратных средств;
- резервное копирование программ и данных;
- обеспечение бесперебойного электропитания и связи;
- обеспечение условий для нормального функционирования серверного и телекоммуникационной оборудования.

1.3 К мерам восстановления работы информационных ресурсов и систем АО «Узнацбанк» относятся:

- задействование резервного оборудования, каналов связи;
- восстановление программ и данных из резервных копий;
- ремонт или замена оборудования;
- переустановка программного обеспечения.

2. Меры обеспечения непрерывной работы

2.1 Плановые профилактические работы проводятся для обеспечения работоспособности и оценки правильности работы основных технических средств: сервер ЛВС АО «Узнацбанк», сервера и системы хранения данных информационных систем, сетевое коммутационное оборудование, средства защиты информации.

2.2 Плановые профилактические работы проводятся специалистами ДИТ, ДИББ, ДРБ, а также Секторов автоматизации, компьютеризации и внедрения ИКТ и Отделов по безопасности, режиму и защите информации областных филиалов и районных филиалов, в обязанности которых входит обслуживание вышеуказанных технических средств (далее – администраторы).

2.3 Плановые профилактические работы должны проводиться не менее одного раза в месяц в отношении следующих технических средств:

- телекоммуникационное оборудование ЛВС и корпоративной сети;
- серверное оборудование ЛВС АО «Узнацбанк», информационных ресурсов и систем, включая установленные на них операционные системы, СУБД и прикладные программы;

- системы хранения данных;

- средства защиты информации.

2.4 Плановые профилактические работы проводятся в соответствии с регламентами обслуживания технических средств.

Профилактическое обслуживание включает в себя:

- проверку целостности настроек и конфигураций;

- анализ системных файлов;

- контроль СУБД;

- проверку отчетности о состоянии и работоспособности, наличие возникших ошибок;

- проверку функционирования основных элементов технических средств;

- проведение диагностики с использованием средств диагностики.

2.5 Ремонтные работы проводятся администраторами для восстановления работоспособности вышедших из строя элементов технических средств или в случае возникновения неполадок.

2.6 Проведение профилактических и ремонтных работ и связанных с ними вскрытий рабочих станций и серверов должны фиксироваться в Журнале вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств, форма которой приведена в приложении к настоящему Плану.

2.7 Администраторы несут ответственность за обеспечение работоспособности обслуживаемых ими технических средств.

2.8 Все важные и критичные информационные системы и ресурсы, обеспечивающие непрерывность работы АО «Узнацбанк», должны быть резервированы.

К таким информационным системам и ресурсам относятся:

1) ИАБС - должна быть предусмотрена организация резервного физического сервера базы данных, системы хранения данных, а также серверов приложений, обеспечивающих доступ сотрудников банка и клиентов, с организацией по возможности работы основного и резервного серверов с распределением нагрузки между ними;

2) БИС - должна быть предусмотрена организация резервного виртуального сервера приложений, сервера базы данных и системы хранения данных, которые будут задействованы при выходе основного оборудования;

3) система электронного документооборота АО «Узнацбанк» - организация резервного сервера на отдельном физическом сервере с организацией по возможности одновременной их работы с распределением нагрузки между ними или задействование резервного сервера при выходе основного сервера;

4) корпоративная электронная почта - организация резервного сервера на отдельном виртуальном сервере с включением его при выходе основного;

5) процессинговая система VISA/MasterCard - организация резервного сервера базы данных и приложений на отдельном физическом сервере с организацией по возможности одновременной их работы с распределением нагрузки между ними или задействование резервного сервера при выходе основного сервера;

6) процессинговая система SWIFT - организация резервного сервера базы данных и приложений на отдельном физическом сервере и задействование резервного сервера при выходе основного сервера;

7) Центр регистрации ключей ЭЦП АО «Узнацбанк» - организация резервного сервера на отдельном физическом сервере с организацией по возможности одновременной их работы с распределением нагрузки между ними или задействование резервного сервера при выходе основного сервера.

Резервирование серверов указанных информационных систем должны обеспечивать администраторы (системные администраторы), обслуживающие данные системы.

2.9 Помимо серверов информационных систем резервированию подлежат следующие технические средства АО «Узнацбанк»:

- маршрутизаторы, используемые для подключения основного ЦОД и головного офиса к внешней и корпоративной сети;
- коммутаторы ядра сети в основном и резервном ЦОД;
- межсетевой экран и средства IDPS, используемые на границе подключения основного ЦОД и головного офиса к внешней сети.

2.10 Резервирование программного обеспечение и данных информационных систем и ресурсов осуществляется в соответствии с Положением по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных, приведенным в приложении №6 к Политике информационной безопасности АО «Узнацбанк».

2.11 Для обеспечения бесперебойного электропитания и связи должны быть предусмотрены следующие меры:

- установка дизель-генератора и источников бесперебойного питания для бесперебойного питания серверного и сетевого оборудования и средств защиты информации в здании головного офиса (основной ЦОД) и отдельно в здании резервного ЦОД;
- использование дополнительных источников бесперебойного питания UPS для серверов, сетевого оборудования, средств защиты информации в основном и резервном ЦОД, коммутационных помещениях областных и районных филиалов.
- организация нескольких каналов подключений к сети Интернет головного офиса (основного ЦОД) от разных операторов телекоммуникаций;
- обеспечение подключение головного офиса, всех областных и районных филиалов к корпоративной сети на базе сети передачи данных EastTelecom и корпоративной сети на базе сети передачи данных Главного центра информатизации Центрального банка;
- организация двух каналов подключений резервного ЦОД к основному ЦОД сети Ethernet и SAN.

2.12 В АО «Узнацбанк» система гарантированного энергоснабжения основного ЦОД должна иметь два входа электропитания от разных подстанций и одну дизельную электростанцию с автоматическим запуском. Все три источника питания должны автоматически подключаться к главному (резервному) фидеру источника питания.

Параметры линий электропередачи, автоматической дизельной электростанции и ее резерв определяются на основе общей мощности, потребляемой оборудованием и системами ЦОД, и должны составлять не менее 10 процентов от резерва мощности.

Дизельная электростанция должна быть с запасом топлива не менее одного дня для бесперебойной работы и запускаться автоматически при отсутствии электричества.

2.13 Основное телекоммуникационное оборудование, базы данных, сервера информационных систем и средства защиты информации АО «Узнацбанк» должны размещаться в серверных комнатах ЦОД.

В областных и районных филиалах серверное и основное телекоммуникационной оборудование должны размещать в отдельных коммутационных помещениях.

Серверные комнаты ЦОД должны обеспечиваться кодовыми замками, системой видеонаблюдения, источниками бесперебойного питания, оборудованы автоматическим газовым огнетушителем, который не подключен к системе пожаротушения здания, а также обеспечены климатическими условиями в соответствии с требованиями O'zDSt 2875: 2014 «Требования к дата-центрам. Обеспечение инфраструктуры и информационной безопасности» и Положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан, утвержденного постановлением Правления Центрального банка Республики Узбекистан от 25 января 2020 года №2/4.

Коммутационные помещения областных и районных филиалах должны обеспечиваться кодовыми замками, системой видеонаблюдения, источниками бесперебойного питания, системой пожарной сигнализации и обеспечения климатических условий.

3. Меры восстановления работы

3.1 В случае возникновения чрезвычайной (аварийной) ситуации восстановление работоспособности информационных систем и ресурсов должно осуществляться по утвержденному аварийному плану восстановления работоспособности (таблица № 1).

3.2 Для каждой информационной системы должен иметься детальный аварийный план восстановления работоспособности. Восстановление информационных систем должно осуществляться сотрудниками ДИТ, ДИББ и ДРБ и иных подразделений в соответствии с детальными планами восстановления. Планы восстановления должны охватывать поведение вовлеченного персонала и подготовленность сотрудников к чрезвычайным ситуациям.

3.3 Мероприятия по восстановлению работоспособности информационных систем и ресурсов в случае аварии предусматривают включение резервных технических средств или ресурсов, замену пришедших в негодность технических средств, восстановление или переустановку программного обеспечения, восстановление информации с архивных копий, либо носителей резервного копирования.

3.4 По утвержденным планам восстановления должны проводиться тренировки не реже двух раз в год. При проведении тренировок все выполненные работы должны документироваться.

Выявленные в ходе тренировок недостатки должны устраняться путем повторного выполнения сотрудниками действий по восстановлению. По результатам тренировок могут вноситься изменения в детальные планы восстановления.

3.5 Для восстановления работоспособности информационных систем и ресурсов должны быть задействованы системы восстановления данных. Сотрудники ДИТ, ДИББ и ДРБ должны проверять состояние системы восстановления данных не реже одного раза в месяц и записывать результаты проверки в специальную книгу. В случае выявления недостатков должен быть составлен акт, в котором указываются выявленные недостатки, меры и сроки устранения этих недостатков.

3.6 В детальных планах восстановления к каждой информационной системы должны быть определены следующие аварийные ситуации и поэтапные меры действий:

1) Отключение электропитания:

Поэтапные меры:

- проверка автоматического включения и работы резервного источника электропитания UPS (предусматривается автоматическое их срабатывание) для серверного оборудования, размещенного в серверном помещении центрального аппарата и филиалов;
- проверка функционирования серверов и сетевого оборудования;
- подключение дизель-генератора и аккумуляторных батарей;
- звонок в РЭС для уточнения причин и требуемого времени восстановления электропитания, вызов при необходимости электрика;
- восстановление подачи основного электропитания, заряд резервных источников электропитания.

2) Пропадание связи (сетевые кабели ЛВС, каналы передачи данных корпоративной сети, подключения к внешней сети и каналы, используемые для интеграции с внешними информационными системами):

Поэтапные меры:

- проверка каналов на всех участках пропавшей связи и работы сетевого оборудования – маршрутизаторов, коммутаторов, состояния сетевого кабеля;
- установление причины сбоя;
- восстановление связи с применением резервного сетевого оборудования или замены сетевого кабеля;
- связь с оператором сети передачи данных в случае пропадания внешней связи подключения к сети Интернет или арендуемого канала корпоративной сети;
- задействование имеющихся резервных каналов связи;
- восстановление полноценной внешней связи;
- ремонт вышедшего из строя сетевого оборудования.

3) Сбой работы серверов:

- контроль работы резервного сервера и сохранности информации (для информационных систем, использующих горячий резерв);

- компилирование данных на резервный сервер для систем с холодным резервом и запуск резервного сервера;

- выяснение причин сбоя - проверка работы серверов и его компонентов, операционной системы, СУБД и прикладных программ (средства диагностики);

- устранение неисправности – замена компонента сервера, восстановление операционной системы из образа, перезапуск или переустановка программы и др.;

- проверка корректной проверки восстановленного сервера и запуск его в эксплуатацию.

Вышеуказанные меры действий должны выполняться ответственными сотрудниками, указанными в таблице №1.

3.7 При проведении восстановительных работ и ликвидации последствий аварийной ситуации должны руководствоваться следующими документами:

- детальный план восстановления информационной системы;

- инструкция по эксплуатации системы восстановления данных;

- инструкции по эксплуатации системы хранения данных, средств связи и защиты информации;

- схема прокладки кабеля внутри здания;

- схема электропитания и подключения дизель-генератора и аккумуляторных батарей;

- план эвакуации из здания в чрезвычайные ситуации;

- договор на оказание услуг, заключенный с оператором сети передачи данных;

- Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности.

4. Меры при чрезвычайных ситуациях

4.1 На случай наступления чрезвычайных ситуаций, вызванных природными и техногенными явлениями, для обеспечения работоспособности информационных систем АО «Узнацбанк» должны быть задействованы ресурсы удаленного резервного ЦОД.

Резервный ЦОД должен отвечать всем требованиям, которые предъявляются к основному ЦОД.

4.2 Данные меры должны быть предусмотрены в отношении информационных систем, указанных в пункте 2.8.

4.3 Резервный ЦОД должен иметь постоянное подключение к корпоративной сети (использование резервных коммутаторов ядра и маршрутизатора в резервном ЦОД) и к внешней сети Интернет (использование резервного маршрутизатора в резервном ЦОД).

4.4 Для полного задействования резервного ЦОД производится:

- переключение сетевого трафика корпоративной сети и внешней сети только на резервный ЦОД (до восстановление основного ЦОД);

- проверка работоспособности и полноты данных серверов баз данных, приложений и системы хранения данных, работающих в горячем резерве;

- задействование свободных ресурсов резервного ЦОД и запуск серверов, находящихся в холодном резерве;

- получение полного управления за средствами обработки, хранения и передачи и защиты информации резервного ЦОД администраторами АО «Узнацбанк» и постоянный контроль с их стороны за функционированием.

5. Регламент обработка инцидентов, аварийных и чрезвычайных ситуаций, взаимодействия со сторонними организациями

5.1 По каждой возникшей аварии и чрезвычайной ситуации дополнительно должны приниматься меры:

- фиксация возникшей ситуации в Журнале учета инцидентов, форма которой приведена в приложении №18 к Политике информационной безопасности АО «Узнацбанк»;

- обработка данных ситуаций, как инцидентов информационной безопасности, в порядке, установленном в разделе 12 Политики информационной безопасности АО «Узнацбанк».

5.2 О каждой возникшей аварии и чрезвычайной ситуации сотрудник, ответственный по инцидентам УИБ ДИББ, обязаны немедленно докладывать начальнику УИБ ДИББ и сообщать администратору информационной безопасности АО «Узнацбанк».

5.3 Сотрудник, ответственный по инцидентам УИБ ДИББ, при наступлении аварийной или чрезвычайной ситуации, а также возникновения инцидентов, указанных в разделе 12 Политики информационной безопасности АО «Узнацбанк», должен взаимодействовать с ГУП «Центр кибербезопасности» в соответствии с Регламентом взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности.

5.4 Начальник УИБ ДИББ о возникших инцидентах информационной безопасности должен информировать Центральный банк Республики Узбекистан в порядке, определенном в постановлении Правления Центрального банка Республики Узбекистан от 25 января 2020 года №2/4 «Об утверждении Положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан».

5.5 В рамках взаимодействия с ГУП «Центр кибербезопасности» сотрудник, ответственный по инцидентам УИБ ДИББ, обязан:

- своевременно, но не позднее 2 (двух) часов после обнаружения инцидента оповещать ГУП «Центр кибербезопасности»;

- в случае принятия оповещения об инциденте от ГУП «Центр кибербезопасности», принимает меры по сохранению целостности и достоверности данных по инциденту;

- предоставить данные по инциденту в ГУП «Центр кибербезопасности», либо оказывает содействие в их получении;

- сообщает ГУП «Центр кибербезопасности» о принятых мерах по предотвращению инцидента;

- оказывает содействие ГУП «Центр кибербезопасности» и принимает участие в расследовании инцидента.

5.5 После получения извещения со стороны ГУП «Центр кибербезопасности», в течение одного дня УИБ ДИББ принимает соответствующие меры для оперативного предотвращения последствий инцидента информационной безопасности, а также обеспечения сохранности данных по инциденту информационной безопасности.

5.6 После принятия необходимых мер по устранению последствий инцидента по истечении 3 (трёх) рабочих дней УИБ ДИББ представляет в ГУП «Центр кибербезопасности» справку об исправлениях официальным письмом с приложением отчета о проделанной работе.

5.7 Работы по восстановлению функционирования и проведению расследований по инцидентам организуются и координируются директором ДИББ.

К расследованию инцидентов информационной безопасности могут привлекаться ГУП «Центр кибербезопасности», а к расследованию инцидентов с тяжкими последствиями с целью привлечения к ответственности нарушителей должны привлекаться правоохранительные органы.

Решение о проведении специального расследования инцидента и привлечение к ним заинтересованных сторон и правоохранительных органов принимается руководством правления АО «Узнацбанк», исходя из тяжести и последствий произошедшего инцидента.

5.7 Если АО «Узнацбанк» инициирует самостоятельное расследование выявленного инцидента информационной безопасности, то по результатам проведенной им работы предоставляется отчет по анализу методов, способов и обстоятельств осуществления инцидентов в отношении принадлежащих ему информационных ресурсов и систем, а также план мер по устранению последствий инцидента информационной безопасности и дальнейшему предотвращению фактов несанкционированного вмешательства в работу информационных ресурсов и систем, с последующей передачей подготовленного отчета в ГУП «Центр кибербезопасности».

5.8 По итогам представления в АО «Узнацбанк» ГУП «Центр кибербезопасности» предложений и рекомендации представленные в виде письма по предотвращению повторного возникновения инцидентов информационной безопасности УИБ ДИББ подготавливается план по их реализации и обеспечивается его исполнение.

Таблица № 1

Аварийный план восстановления работоспособности

Наименование аварии или сбоя	Этапы действий	Время выполнения*	Ответственный
1. Отключение (полное или частичное) электропитания			
Отключение электропитания головного офиса и основного ЦОД	1) доклад директору ДИТ, ДИББ; 2) взаимодействие с подразделением административно-хозяйственного обеспечения, звонок в РЭС для уточнения причин и требуемого времени восстановления, вызов электрика при необходимости, 3) проверка включения и работы резервного источника электропитания UPS (предусматривается автоматическое их срабатывание) серверов, сетевого оборудования и средств защиты; 4) проверка автоматического включения дизель-генератора в здании; 5) проверка и контроль функционирования основных серверов, сетевого оборудования и средств защиты в период работы альтернативного источника электропитания; 6) восстановление подачи основного электропитания, заряд резервных источников электропитания.	1-5 минут 1-5 минут 1-5 минут 1-5 минут 1 и более минут 1 и более часов	Администраторы ДИТ и ДИББ, подразделение административно-хозяйственного обеспечения

Отключение электропитания резервного ЦОД	1) доклад директору ДРБ; 2) взаимодействие с подразделением административно-хозяйственного обеспечения, звонок в РЭС для уточнения причин и требуемого времени восстановления, вызов электрика при необходимости, 3) проверка включения и работы резервного источника электропитания UPS (предусматривается автоматическое их срабатывание) серверов, сетевого оборудования и средств защиты; 4) проверка автоматического включения дизель-генератора в здании; 5) проверка и контроль функционирования основных серверов, сетевого оборудования и средств защиты в период работы альтернативного источника электропитания; 6) восстановление подачи основного электропитания, заряд резервных источников электропитания.	1-5 минут 1-5 минут 1-5 минут 1-15 минут 1 и более минут 1 и более часов	Администраторы ДРБ, подразделение административно-хозяйственного обеспечения
Отключение электропитания в областных и районных филиалах	1) доклад начальнику Сектора автоматизации, Отдела безопасности; 2) взаимодействие с подразделением административно-хозяйственного обеспечения, звонок в РЭС для уточнения причин и требуемого времени восстановления, вызов электрика при необходимости, 3) проверка включения и работы резервного источника электропитания UPS серверов, сетевого оборудования и средств защиты; 4) проверка и контроль функционирования основных серверов, сетевого оборудования и средств защиты в период работы альтернативного источника электропитания или их безопасное отключение на случай длительного пропадания электроэнергии; 5) восстановление подачи основного электропитания, заряд резервных источников электропитания.	1-5 минут 5-10 минут 1-5 минут 1 и более минут 1 и более часов	Сектор автоматизации, компьютеризации и внедрения ИКТ, Отдел по безопасности, режиму и защите информации, подразделение административно-хозяйственного обеспечения

2. Повреждение связи			
Повреждение подключения к внешней сети (головной офис, основной ЦОД, резервный ЦОД)	1) доклад директору ДИТ (ДИББ, ДРБ); 2) проверка внешних каналов связи (выход на оператора телекоммуникаций), работы сетевого оборудования – маршрутизаторов, коммутаторов, прокси-сервера, межсетевого экрана, состояния сетевого кабеля (выяснение причин сбоя); 3) восстановление связи с применением (задействованием) резервного оборудования или замены сетевого кабеля; 4) переключение трафика на работающие внешние каналы связи (изменение таблицы маршрутизации в маршрутизаторе); 5) постоянная связь с оператором телекоммуникаций в случае пропадания внешней связи для контроля хода восстановления связи; 6) ремонт оборудования, вышедшего из строя или приобретение нового, возврат старых настроек маршрутизатора, восстановление полноценной связи.	1-10 минут 5-20 минут 10-20 минут 10-20минут В период пропадания связи После восстановления связи	Администраторы ДИТ, ДИББ, ДРБ, сетевой администратор корпоративной сети
Повреждение подключения к корпоративной сети (головной офис, основной ЦОД, резервный ЦОД)	1) доклад директору ДИТ (ДИББ, ДРБ); 2) проверка каналов подключения к корпоративной сети (выход на оператора телекоммуникаций), работы сетевого оборудования – маршрутизаторов, коммутаторов, состояния сетевого кабеля (выяснение причин сбоя); 3) восстановление связи с применением (задействованием) резервного сетевого оборудования или замены сетевого кабеля; 4) переключение на работу на одну из работающих корпоративных сетей ГЦИ или EastTelecom (внесение изменений в таблицу маршрутизации); 5) постоянная связь с оператором телекоммуникаций в случае пропадания связи на его сети для контроля хода восстановления связи; 6) ремонт оборудования, вышедшего из строя или приобретение нового, возврат старых настроек маршрутизации, восстановление полноценной связи.	1-10 минут 5-20 минут 10-20 минут 10-20 минут В период пропадания связи После восстановления связи	Администраторы ДИТ, ДИББ, ДРБ, сетевой администратор корпоративной сети

Повреждение подключения областных и районных филиалов к корпоративной сети	1) доклад начальнику Сектора автоматизации, Отдела безопасности; 2) доклад сетевому администратору корпоративной сети и директору ДИТ; 3) проверка каналов связи (выход на ГЦИ и EastTelecom), работы сетевого оборудования – маршрутизаторов, коммутаторов, состояния сетевого кабеля в филиале (выяснение причин сбоя); 4) переключение на работу на одну из работающих корпоративных сетей ГЦИ или EastTelecom центрального аппарата, регионального филиала или отделения банка в случае сбоя связи на одной из корпоративных сетей (внесение изменений в таблицу маршрутизации); 5) восстановление связи с применением резервного сетевого оборудования или замены сетевого кабеля, в случае их сбоев внутри филиала; 6) постоянная связь с оператором телекоммуникаций в случае пропадания связи на его сети для контроля хода восстановления связи; 7) ремонт оборудования, вышедшего из строя или приобретение нового, возврат старых настроек маршрутизации, восстановление полноценной связи.	5-10 минут 5-10 минут 10-20 минут 20-30 минут 20-30 минут В период пропадания связи После восстановления связи	Сектор автоматизации, компьютеризации и внедрения ИКТ, Отдел по безопасности, режиму и защите информации, сетевой администратор корпоративной сети
3. Сбой работы серверов информационных систем			
Сбой работы серверов приложений и базы данных (выход из строя физического компонента сервера – процессор, ОЗУ, материнской платы, сетевой карты и др.)	1) доклад начальнику Департамента; 2) контроль работы резервного сервера и сохранности информации (для информационных систем, использующих горячий резерв); 3) компилирование данных на резервный сервер для систем с холодным резервом и запуск резервного сервера; 4) установление причин сбоя вышедшего из строя сервера; 5) ремонт вышедшего из строя сервера или замена вышедшего из строя компонента; 6) восстановление работы вышедшего из строя сервера; 7) восстановление данных на основном сервере (если не используется единая система хранения) и запуск сервера.	5-10 минут 5-10 минут 10-30 минут 10-30 минут от 1 часа до 2 суток от 1 часа до 2 суток от 1 часа до 2 суток	Системные администраторы

Сбой работы системного или прикладного программного обеспечения	1) доклад начальнику Департамента; 2) контроль работы резервного сервера и сохранности информации (для информационных систем, использующих горячий резерв); 3) компилирование данных на резервный сервер для систем с холодным резервом и запуск резервного сервера; 4) установление причин сбоя вышедшего из строя сервера; 5) восстановление системной программы с использования образа или переустановка прикладной программы на сервере, где произошел сбой; 6) восстановление работы вышедшего из строя сервера; 7) восстановление данных на основном сервере (если не используется единая система хранения) и запуск сервера.	5-10 минут 5-10 минут 10-30 минут 10-30 минут 1-2 часа 1-2 часа 1-2 часа	Системные администраторы
4. Сбой работы официального веб-сайта			
Отключение (полное или частичное) электропитания Повреждение связи, Сбой работы сервера, Сбой работы программного обеспечения	Мероприятия по восстановлению официального веб-сайта при указанных сбоях должны производиться ООО «AB Digital», на хостинг-площадке которого размещен веб-ресурс в соответствии с заключенным с ним договором. Действия Народного банка: 1) доклад начальнику Департамента информационных технологий; 2) взаимодействие с ответственным в ООО «AB Digital», выяснение причин; 3) проверка работоспособности, полноты информации и восстановления работы официального веб-сайта.	5-10 минут 5-10 минут 15-30 минут после восстановления	Департамент развития сети и сервиса банка

Примечание:

1)в графе «Время выполнения» указывается время с момента возникновения и обнаружения аварии.

Приложение
к Плану обеспечения непрерывной
работы и восстановления
работоспособности в чрезвычайных
(аварийных) ситуациях

Журнал вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств

№	Дата	Событие	Подпись ответственного

Приложение №18
к Политике информационной
безопасности АО «Узнацбанк»
№ 124. 2 27.12.2021г

Журнал учета инцидентов информационной безопасности

№ п/п	Дата и время возникновения инцидента	Наименование объекта защиты, на котором произошел инцидент (место возникновения)	Вид и способ реализации угрозы	Характер последствий	Принятые действия и меры	Дата и время ликвидации

Приложение №19
к Политике информационной
безопасности АО «Узнацбанк»
№ 124-б 27.12.2021

Журнал ознакомления с Политикой информационной безопасности

№	Ф.И.О.	Подразделение (отдел)/должность	Дата	Подпись