Утверждено приказом Генерального директора
ООО МКК «Экофинанс»
от «10» февраля 2026 г.

_____А.А. Клейменова

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Общества с ограниченной ответственностью
микрокредитная компания «Экофинанс»

г. Москва
2026 год

ОГЛАВЛЕНИЕ

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее Политика) разработана Обществом с ограниченной ответственностью микрокредитная компания «Экофинанс» (ООО МКК «Экофинанс») (далее – Организация) и регламентирует порядок обеспечения защиты получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых Организацией, информации Организации (далее соответственно автоматизированные системы, защищаемая информация, защита информации).

1.2. Политика разработана в соответствии с:

- «Положением об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (утв. Банком России 17.04.2019 № 684-П).
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее ГОСТ Р 57580.1-2017).
- Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее Постановление № 1119).
- статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (далее РС БР ИББС-2.22-009).
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.7-2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности» (далее РС БР ИББС-2.7-2015), и иными нормативными правовыми актами.

1.3. Настоящая Политика распространяется на все бизнес-процессы Организации и обязательна для применения всеми работниками и руководством Организации.

1.4. Настоящая политика распространяется на информационные системы Организации.

1.5. Лица, осуществляющие разработку внутренних документов Организации, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

1.6. Термины, используемые в настоящей Политике, применяются в тех значениях, которые определены в законодательстве, нормативных правовых актах, указанных в настоящей Политике, в частности в указанном выше ГОСТ Р 57580.1-2017, а также:

ИБ – информационная безопасность;

АС – автоматизированная система;

СА – системный администратор, подразделение, работники которого являются системными администраторами, подразделение, отвечающее за информационную безопасность Организации, и его работники (при наличии);

ПДн – персональные данные;

СИБ, СОИБ – система обеспечения информационной безопасности;

ПО – программное обеспечение;

ЭЦП – электронно-цифровая подпись;

НСД – несанкционированный доступ;

ИС – информационная система;

УБД – угрозы базам данных;

АРМ – автоматизированное рабочее место;

ГЛАВА 2. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Защита информации согласно настоящей Политике регламентирована в целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью 1 статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

2.2. Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков информационной безопасности (ИБ).

2.3. Для достижения основной цели обеспечивается эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСТЭК России, Банка России и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников;
- повышение деловой репутации и корпоративной культуры.

2.2. В случае если защищаемая информация содержит персональные данные, предпринимаются меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Федеральный закон «О персональных данных»).

ГЛАВА 3. ОСНОВНЫЕ ТИПЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

3.1. При идентификации и учете объектов информатизации Организацией учитываются следующие основные уровни информационной инфраструктуры:

а) системные уровни:

- уровень аппаратного обеспечения;
- уровень сетевого оборудования;
- уровень сетевых приложений и сервисов;
- уровень серверных компонентов виртуализации, программных инфраструктурных сервисов;
- уровень операционных систем, систем управления базами данных, серверов приложений;

б) уровень АС и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес-процессов или технологических процессов Организации.

3.2. Организация осуществляет защиту следующей информации:

- информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронной форме работниками Организации и (или) клиентами (далее электронные сообщения);
- информации, необходимой Организации для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информации об осуществленных Организацией и его клиентами финансовых операциях.
- резервных копий ресурсов доступа, баз данных и архивных хранилищ информации;
- информации, обрабатываемой на виртуальных машинах, а также при реализации технологии виртуализации.
- а также иные виды информации, обязанность по защите которых установлена действующим законодательством, договорными отношениями или решением руководства Организации.

3.3. В составе основных типов ресурсов доступа:

- АС;
- базы данных;
- сетевые файловые ресурсы;

− виртуальные машины, предназначенные для размещения серверных компонентов АС;
− виртуальные машины, предназначенные для размещения АРМ пользователей и эксплуатационного персонала;
− ресурсы доступа, относящиеся к WEB-сервисам Организации в сетях Интранет и Интернет.

3.4. В составе основных типов объектов доступа:
− автоматизированные рабочие места (АРМ) пользователей;
− АРМ эксплуатационного персонала;
− серверное оборудование;
− сетевое оборудование;
− системы хранения данных;
− аппаратные модули безопасности (HSM);
− устройства печати и копирования информации;
− виртуальные машины, предназначенные для размещения АРМ пользователей и эксплуатационного персонала;
– ресурсы доступа, относящиеся к сервисам электронной почты;
– ресурсы доступа, относящиеся к WEB-сервисам Организации в сетях Интранет и Интернет.

ГЛАВА 4. ОСНОВНЫЕ ПРИНЦИПЫ И ПРИОРИТЕТЫ ВЫБОРА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И СИСТЕМЫ ОРГАНИЗАЦИИ И УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ

РАЗДЕЛ 4.1. ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ТРЕБОВАНИЯ К СОДЕРЖАНИЮ БАЗОВОГО СОСТАВА КОТОРЫХ УСТАНОВЛЕНЫ В РАЗДЕЛЕ 7 ГОСТ Р 57580.1-2017

4.1.1. Выбор и применение Организацией мер защиты информации включает:
− выбор мер защиты информации, требования к содержанию базового состава которых установлены в разделе 7 ГОСТ Р 57580.1-2017, в соответствии с уровнем защиты информации Организации, определенным в соответствии с настоящей Политикой;
− адаптацию (уточнение) при необходимости выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации Организации и структурно-функциональных характеристик объектов информатизации, в том числе АС, включаемых в область применения ГОСТ Р 57580.1-2017;
− исключение из базового состава мер, не связанных с используемыми информационными технологиями;
− дополнение при необходимости адаптированного (уточненного) состава и содержания мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;
− применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации в соответствии с положениями разделов 8 и 9 ГОСТ Р 57580.1-2017.

4.1.2. Применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации включает:
− применение на различных уровнях информационной инфраструктуры выбранных Организацией мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации, требования к содержанию базового состава которых установлены в разделе 7 ГОСТ Р 57580.1-2017;
− применение выбранных Организацией мер защиты информации, обеспечивающих приемлемые для Организации полноту и качество защиты информации, входящих в систему организации и управления защитой информации, требования к содержанию базового состава которых установлены в разделе 8 ГОСТ Р 57580.1-2017;
− применение выбранных Организацией мер защиты информации, направленных на обеспечение защиты информации на всех стадиях жизненного цикла АС и приложений, требования к содержанию базового состава которых установлены в разделе 9 ГОСТ Р 57580.1-2017;
− оценку остаточного операционного риска (финансового эквивалента возможных потерь), вызванного неполным или некачественным выбором и применением мер защиты информации, требования к содержанию базового состава которых установлены в разделах 7, 8, 9 ГОСТ Р 57580.1-2017, и обработку указанного риска в соответствии с процедурой, определенной требованиями

нормативных актов Банка России в соответствии с рекомендациями по оценке рисков информационной безопасности, приведенными в РС БР ИББС-2.2-2009 и РС БР ИББС-2.7-2015.

4.1.3. Принципы и приоритеты выбора организационных и технических мер системы защиты информации и системы организации и управления защитой информации Организации определяются видами угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных Организации, в том числе:

- угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;
- угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
- угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
- угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
- угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

4.1.4. Для противостояния угрозам безопасности информации и их влиянию на операционный риск Организация обеспечивает необходимый и достаточный уровень защиты информации, а также сохраняет этот уровень при изменении условий как внутри, так и вне Организации.

РАЗДЕЛ 4.2. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИЕЙ

4.2.1. Определение уровня защиты информации Организация осуществляет ежегодно не позднее первого рабочего дня календарного года определения уровня защиты.

4.2.2. ГОСТ Р 57580.1-2017 определяет три уровня защиты информации:

- уровень 3 минимальный;
- уровень 2 стандартный;
- уровень 1 усиленный.

4.2.3. В Организации формируется один контур безопасности.

4.2.4. Уровень защиты информации Организации для контура безопасности устанавливается нормативными актами Банка России на основе:

- объема финансовых операций;
- размера Организации, отнесения Организации к категории малых предприятий и микропредприятий;
- значимости Организации для финансового рынка и национальной платежной системы.

4.2.5. Определение типа угроз безопасности персональных данных, актуальных для информационной системы персональных данных, производится оператором информационной системы персональных данных в соответствии с пунктом 7 Постановления № 1119, то есть СА.

4.2.6. При обеспечении защиты информации, содержащей персональные данные, под

актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

4.2.7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится ООО МКК «Экофинанс» с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

4.2.8. С учетом специфики обработки и обеспечения безопасности персональных данных в Организации, угрозы утечки персональных данных по техническим каналам, а также угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в АС, признаются неактуальными.

4.2.9. Для информационной системы Организации актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Организация не использует средства криптографической защиты информации (СКЗИ).

4.2.10. Для обеспечения соответствия 4му уровню защищенности персональных данных при их обработке в АС, используются требования, установленные ГОСТ Р 57580.12017 для уровня 3 минимальный.

ГЛАВА 5. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ СОГЛАСНО ГОСТ Р 57580.12017

РАЗДЕЛ 5.1. ОБЩИЕ ПОЛОЖЕНИЯ

5.1.1. Реализация требований к содержанию базового состава мер защиты информации для следующих уровней защиты информации, установленных ГОСТ Р 57580.12017, используется Организацией для обеспечения выполнения требований к защите персональных данных при их обработке в информационных системах персональных данных (АС) при появлении угрозы защищенности:

- для обеспечения соответствия четвертому уровню защищенности персональных данных при их обработке в АС рекомендуется использовать требования, установленные ГОСТ Р 57580.12017 для уровня 3 минимальный;
- для обеспечения соответствия третьему и второму уровням защищенности персональных данных при их обработке в АС рекомендуется использовать требования, установленные ГОСТ Р 57580.12017 для уровня 2 стандартный;
- для обеспечения соответствия первому уровню защищенности персональных данных при их обработке в АС рекомендуется использовать требования, установленные ГОСТ Р 57580.12017 для уровня 1 усиленный.

Справочная информация по составу и содержанию рекомендуемых организационных мер, подлежащих реализации Организацией в связи с обработкой ПДн в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152 ФЗ "О персональных данных", приведена в приложении Б к ГОСТ Р 57580.12017.

5.1.2. При проведении работ по предоставлению доступа к защищаемой информации Организация руководствуется следующими принципами, установленными для рынка финансовых услуг в ГОСТ Р ИСО/ТО 13569:

- "знать своего клиента": принцип, реализация которого в основном направлена на обладание информацией в отношении благонадежности клиента, его основных потребностей, отсутствия его незаконной или нелегальной деятельности;
- "знать своего работника": принцип, реализация которого в основном направлена на обладание информацией об отношении работников Организации к своим служебным обязанностям, наличии у них возможных проблем, в том числе финансовых, имущественных или личных, которые могут потенциально привести к действиям, направленным на нарушение требований к защите информации;

− "необходимо знать": принцип, реализация которого в основном направлена на ограничение прав логического и (или) физического доступа работников Организации на уровне, минимально необходимом для выполнения служебных обязанностей;

− "двойное управление": принцип, реализация которого в основном направлена на сохранение целостности и неизменности информации путем дублирования (алгоритмического, временного, ресурсного или иного) действий субъектов доступа в рамках реализации финансовых операций и транзакций, выполняемого до их окончательного завершения.

5.1.3. Организация обеспечивает автоматизацию предоставляемых финансовых услуг, бизнес-процессов, технологических процессов и (или) обработку защищаемой информации с использованием АС и приложений, создаваемых (модернизируемых) Организацией самостоятельно и (или) с привлечением сторонних организаций.

Обязанность обеспечения Организацией автоматизации бизнес-процессов, технологических процессов и (или) обработки защищаемой информации только с применением АС устанавливается требованиями нормативных актов Банка России.

5.1.4. Организация самостоятельно определяет необходимость использования средств криптографической защиты информации (СКЗИ), если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации, в том числе нормативными актами Банка России, стандартами, правилами профессиональной деятельности, и (или) правилами платежной системы.

5.1.5. Юридические лица или индивидуальные предприниматели, привлекаемые Организацией для проведения работ по обеспечению защиты информации, должны иметь лицензию на деятельность по технической защите конфиденциальной информации.

РАЗДЕЛ 5.2. ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ СОГЛАСНО ГОСТ Р 57580.12017

5.2.1. Общие положения

5.2.1.1. РАЗДЕЛ 7 ГОСТ Р 57580.12017 устанавливает требования к содержанию базового состава мер защиты информации для следующих процессов (направлений) защиты информации:

а) процесс 1 «Обеспечение защиты информации при управлении доступом»:

− управление учетными записями и правами субъектов логического доступа;

− идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;

− защита информации при осуществлении физического доступа;

− идентификация, классификация и учет ресурсов и объектов доступа;

б) процесс 2 «Обеспечение защиты вычислительных сетей»:

− сегментация и межсетевое экранирование вычислительных сетей;

− выявление сетевых вторжений и атак;

− защита информации, передаваемой по вычислительным сетям;

− защита беспроводных сетей;

в) процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»;

г) процесс 4 «Защита от вредоносного кода»;

д) процесс 5 «Предотвращение утечек информации»;

е) процесс 6 «Управление инцидентами защиты информации»:

− мониторинг и анализ событий защиты информации;

− обнаружение инцидентов защиты информации и реагирование на них;

ж) процесс 7 «Защита среды виртуализации»;

и) процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

5.2.1.2. Меры защиты информации, входящие в систему защиты информации, реализуются:

− в соответствии с положениями разделов 6, 8, 9 ГОСТ Р 57580.12017;

− с ограничениями и условиями, определенными в разделе 6 ГОСТ Р 57580.12017, обусловленными технической возможностью и экономической целесообразностью (рискаппетитом) Организации.

5.2.1.3 В случае возникновения в информационной инфраструктуре Организации зафиксированных нештатных ситуаций (аварий или существенного снижения функциональности компонентов информационной инфраструктуры), при которых временно отсутствует техническая возможность применения всех мер защиты информации, входящих в систему защиты информации,

Организация предусматривает осуществление ответственными работниками действий, направленных на выполнение своих служебных обязанностей в условиях отсутствия применения отдельных мер защиты информации, а также должный контроль указанных действий.

5.2.1.4 Меры защиты информации, входящие в систему защиты информации, реализуются в том числе для обеспечения защиты:

- резервных копий ресурсов доступа, баз данных и архивных хранилищ информации;
- информации, обрабатываемой на виртуальных машинах, а также при реализации технологии виртуализации.

5.2.1.5. При формировании данных регистрации о событиях защиты информации, предусмотренных ГОСТ Р 57580.12017 (рекомендуемый для выявления, регистрации и анализа перечень событий защиты информации установлен в приложении В ГОСТ Р 57580.12017), для каждого фиксируемого действия и (или) операции определяется следующий набор параметров:

- данные, позволяющие идентифицировать выполненное действие или операцию;
- дата и время осуществления действия или операции;
- результат выполнения действия или операции (успешно или неуспешно);
- идентификационные данные субъекта доступа, выполнившего операцию;
- идентификационные данные ресурса доступа, в отношении которого выполнена операция;
- идентификационные данные, используемые для адресации объекта доступа, который использовался субъектами доступа для выполнения операции.

5.2.2. Процесс 1 «Обеспечение защиты информации при управлении доступом»

Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

Применяемые Организацией меры по управлению учетными записями и правами субъектов логического доступа обеспечивают:

- организацию и контроль использования учетных записей субъектов логического доступа;
- организацию и контроль предоставления (отзыва) и блокирования логического доступа;
- регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

При реализации подпроцесса «Управление учетными записями и правами субъектов логического доступа» используется ГОСТ Р 50739.

5.2.3. Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»

5.2.3.1. Применяемые Организацией меры по идентификации, аутентификации, авторизации (разграничению доступа) при осуществлении логического доступа обеспечивают:

- идентификацию и аутентификацию субъектов логического доступа;
- организацию управления и организацию защиты идентификационных и аутентификационных данных;
- авторизацию (разграничение доступа) при осуществлении логического доступа;
- регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

При реализации подпроцесса «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» используется ГОСТ Р 50739.

5.2.3.2. Применяемые Организацией меры по защите информации при осуществлении физического доступа обеспечивают:

- организацию и контроль физического доступа в помещения, в которых расположены объекты доступа (далее помещения);
- организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах (далее общедоступные объекты доступа);
- регистрацию событий, связанных с физическим доступом.

5.2.3.3 При реализации подпроцесса «Идентификация и учет ресурсов и объектов доступа» Организация вправе использовать ГОСТ Р 50739.

5.2.3.4. Применяемые Организацией меры по идентификации и учету ресурсов и объектов доступа обеспечивают:

− организацию учета и контроль состава ресурсов и объектов доступа;
− регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.

5.2.4. Процесс 2 «Обеспечение защиты вычислительных сетей»

5.2.4.1 Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»

Применяемые Организацией меры по сегментации и межсетевому экранированию вычислительных сетей обеспечивают:
− сегментацию и межсетевое экранирование внутренних вычислительных сетей;
− защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет;
− регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.

При реализации подпроцесса «Сегментация и межсетевое экранирование вычислительных сетей» Организация вправе использовать ГОСТ Р ИСО/МЭК 270331.

5.2.4.2. Подпроцесс «Выявление вторжений и сетевых атак»

Применяемые Организацией меры по выявлению вторжений и сетевых атак обеспечивают:
− мониторинг и контроль содержимого сетевого трафика;
− регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.

При реализации подпроцесса «Выявление вторжений и сетевых атак» Организация вправе использовать Требования к системам обнаружения вторжений, утвержденные Приказом ФСТЭК России
от 6 декабря 2011 г. № 638.

5.2.4.3. Подпроцесс «Защита информации, передаваемой по вычислительным сетям»

Организация применяет меры по защите информации, передаваемой по вычислительным сетям.

5.2.4.4. Подпроцесс «Защита беспроводных сетей»

Применяемые Организацией меры по защите беспроводных сетей обеспечивают:
− защиту информации от раскрытия и модификации при использовании беспроводных сетей;
− защиту внутренних вычислительных сетей при использовании беспроводных сетей;
− регистрацию событий защиты информации, связанных с использованием беспроводных сетей.

5.2.5. Процесс 4 «Защита от вредоносного кода»

Применяемые Организацией меры по защите от вредоносного кода обеспечивают:
− организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры;
− организацию и контроль применения средств защиты от вредоносного кода;
− регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.

При реализации процесса «Защита от вредоносного кода» Организация вправе использовать Требования к средствам антивирусной защиты, утвержденные Приказом ФСТЭК России от 20 марта 2012 г. № 28.

5.2.6. Процесс 5 «Предотвращение утечек информации»

Применяемые Организацией меры по предотвращению утечек информации обеспечивают:
− блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;
− контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;
− регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.

Рекомендации, обеспечивающие снижение рисков утечки информации путем мониторинга и контроля информационных потоков, приведены в Рекомендациях в области стандартизации Банка

России РС БР ИББС2.92016 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации.

5.2.7. Процесс 6 «Управление инцидентами защиты информации»

5.2.7.1 Подпроцесс «Мониторинг и анализ событий защиты информации»

Применяемые Организацией меры по мониторингу и анализу событий защиты информации обеспечивают:

- организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта;
- сбор, защиту и хранение данных регистрации о событиях защиты информации;
- анализ данных регистрации о событиях защиты информации;
- регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.

При реализации подпроцесса «Мониторинг и анализ событий защиты информации» Организация вправе использовать ГОСТ Р ИСО/МЭК ТО 18044.

Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в Рекомендациях в области стандартизации Банка России РС БР ИББС2.52014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности.

5.2.7.2 Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»

Применяемые Организацией меры по обнаружению инцидентов защиты информации и реагирование на них обеспечивают:

- обнаружение и регистрацию инцидентов защиты информации;
- организацию реагирования на инциденты защиты информации;
- организацию хранения и защиту информации об инцидентах защиты информации;
- регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.

При реализации подпроцесса «Обнаружение инцидентов защиты информации и реагирование на них» Организация вправе использовать ГОСТ Р ИСО/МЭК ТО 18044.

Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в Рекомендациях в области стандартизации Банка России РС БР ИББС2.52014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности.

5.2.8. Процесс 7 «Защита среды виртуализации»

5.2.8.1 Для обеспечения должного уровня защиты информации при использовании технологии виртуализации, организационные и технические меры, применяемые для защиты среды виртуализации, являются дополнительными и применяются в совокупности с иными мерами защиты информации, установленными ГОСТ Р 57580.12017.

Дополнительные организационные и технические меры, применяемые для защиты среды виртуализации, определяются для следующих процессов (подпроцессов) защиты информации, перечисленных в 7.1.1 ГОСТ Р 57580.12017:

- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
- сегментация и межсетевое экранирование вычислительных сетей.

5.2.8.2. Применяемые Организацией меры по защите среды виртуализации обеспечивают:

- организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации;
- организацию и контроль информационного взаимодействия и изоляции виртуальных машин;
- организацию защиты образов виртуальных машин;

− регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.

Рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации в рамках реализации технологических процессов приведены в Рекомендациях в области стандартизации Банка России РС БР ИББС2.82015 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации и ГОСТ Р 56938.

5.2.9. Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

Применяемые Организацией меры по защите информации при осуществлении удаленного логического доступа работников Организации с использованием мобильных (переносных) устройств обеспечивают:

− защиту информации от раскрытия и модификации при осуществлении удаленного доступа;

− защиту внутренних вычислительных сетей при осуществлении удаленного доступа;

− защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.

РАЗДЕЛ 5.3. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ

5.3.1. Общие положения

5.3.1.1 Разделы 8 и 9 ГОСТ Р 57580.12017 устанавливают требования к содержанию базового состава мер защиты информации, входящих в состав системы организации и управления защитой информации, направленных на обеспечение должной полноты и качества реализации системы защиты информации.

5.3.1.2 Меры системы организации и управления защитой информации применяются:

− на системных уровнях информационной инфраструктуры;

− на этапах жизненного цикла АС и приложений, используемых для обработки, передачи и (или) хранения защищаемой информации в рамках выполнения и (или) обеспечения выполнения бизнес-процессов или технологических процессов Организации.

5.3.1.4 Меры системы организации и управления защитой информации на системных уровнях применяются в рамках следующих направлений защиты информации:

− направление 1 «Планирование процесса системы защиты информации» («Планирование»);

− направление 2 «Реализация процесса системы защиты информации» («Реализация»);

− направление 3 «Контроль процесса системы защиты информации» («Контроль»);

− направление 4 «Совершенствование процесса системы защиты информации» («Совершенствование»).

5.3.2. Направление 1 «Планирование процесса системы защиты информации»

5.3.2.1 В рамках направления «Планирование» Организация обеспечивает определение (пересмотр):

− области применения процесса системы защиты информации;

− состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.12017;

− состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.12017, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;

− порядка применения мер защиты информации в рамках процесса системы защиты информации.

Реализация деятельности в рамках направления «Планирование» осуществляется на основе политики Организации в отношении целевых показателей величины допустимого остаточного операционного риска (риск аппетита), связанного с обеспечением безопасности информации, а также при необходимости на основе результатов деятельности в рамках направления «Совершенствование».

Рекомендации по документированию деятельности в области обеспечения информационной безопасности приведены в Рекомендациях в области стандартизации Банка России РС БР ИББС2.02007

Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС1.0.

5.3.3. Направление 2 «Реализация процесса системы защиты информации»

5.3.3.1 Деятельность в рамках направления «Реализация» выполняется по результатам выполнения направлений «Планирование» и (или) «Совершенствование».

В рамках направления «Реализация» Организация обеспечивает:

- должное применение мер защиты информации;
- определение ролей защиты информации, связанных с применением мер защиты информации;
- назначение ответственных лиц за выполнение ролей защиты информации;
- доступность реализации технических мер защиты информации;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия [в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности], в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации Организации;
- обучение, практическую подготовку (переподготовку) работников Организации, ответственных за применение мер защиты информации;
- повышение осведомленности (инструктаж) работников в области защиты информации.

Рекомендации по определению потребностей организации в ресурсах, необходимых для реализации процессов информационной безопасности, и по проведению контроля эффективности использования этих ресурсов приведены в Рекомендации в области стандартизации Банка России РС БР ИББС2.72015.

5.3.4. Направление 3 «Контроль процесса системы защиты информации»

5.3.4.1 Деятельность в рамках направления «Контроль» обеспечивает уверенность в том, что применение мер защиты информации осуществляется надлежащим образом и соответствует политике Организации в отношении целевых показателей величины допустимого остаточного операционного риска (рискаппетита), связанного с обеспечением безопасности информации.

Применяемые Организацией меры защиты информации обеспечивают контроль:

- области применения процесса системы защиты информации;
- должного применения мер защиты информации в рамках процесса системы защиты информации;
- знаний работников в части применения мер защиты информации.

5.3.5. Направление 4 «Совершенствование процесса системы защиты информации»

5.3.5.1 Деятельность в рамках направления «Совершенствование» выполняется на основе результатов проведения мероприятий по обнаружению инцидентов защиты информации и реагированию на них, обнаружению недостатков в обеспечении защиты информации в рамках направления «Контроль», а также в случаях изменения политики Организации в отношении принципов и приоритетов в реализации системы защиты информации, целевых показателей величины допустимого остаточного операционного риска (рискаппетита).

Применяемые Организацией меры в рамках направления «Совершенствование» обеспечивают формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотр применяемых мер защиты информации. При этом непосредственная деятельность по совершенствованию процесса защиты информации выполняется в рамках направления «Реализация» и при необходимости направления «Планирование».

РАЗДЕЛ 5.4. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

5.4.1. Деятельность по защите информации на стадиях жизненного цикла АС реализуется путем:

- размещения компонентов АС в защищенной информационной инфраструктуре, для которой на системных уровнях реализованы процессы системы защиты информации, определенные в разделе 7 ГОСТ Р 57580.12017;

− создания и обеспечения применения системы защиты информации для конкретной АС, реализующей отдельные дополнительные (по отношению к требованиям раздела 8 настоящего стандарта) функции защиты информации для АС, не реализованные на системных уровнях.

5.4.2. Применяемые Организацией меры на этапах жизненного цикла АС обеспечивают:

− определение состава мер защиты информации, реализуемых в АС (мер системы защиты информации АС);

− должное применение и контроль применения мер системы защиты информации АС;

− контроль отсутствия уязвимостей защиты информации в прикладном ПО АС и информационной инфраструктуре, предназначенной для размещения АС;

− конфиденциальность защищаемой информации.

Рекомендации по обеспечению информационной безопасности на стадиях жизненного цикла АС приведены в Рекомендациях в области стандартизации Банка России РС БР ИББС2.72015.

РАЗДЕЛ 5.5. СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ МЕР, СВЯЗАННЫХ С ОБРАБОТКОЙ ОРГАНИЗАЦИЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Б.1 Цели обработки ПДн в ООО МКК «Экофинанс» документально установлены и утверждены руководством Организации.

Б.2 В Организации при изменении требований законодательства РФ будет осуществлено уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн и организована деятельность по своевременному направлению указанного уведомления в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

Б.3 В Организации установлены критерии отнесения АС к информационным системам персональных данных (АС).

Б.4 В Организации определены, выполняются, регистрируются и контролируются процедуры учета ресурсов ПДн, в том числе учета АС.

Для каждого ресурса ПДн обеспечено:

установление цели обработки ПДн;

установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;

выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками Организации;

выполнение ограничения обработки ПДн достижением цели обработки ПДн;

соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;

точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;

выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн в случае, если получение такого согласия необходимо в соответствии с требованиями закона;

выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам в случае, если получение такого согласия необходимо в соответствии с требованиями закона;

прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных законом, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

Б.5 В Организации определены, выполняются, регистрируются и контролируются процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные законом, в следующих случаях:

− по достижении цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн);

− отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн);

− если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

− выявления неправомерной обработки ПДн, осуществляемой Организацией или обработчиком, действующим по его поручению, если обеспечить правомерность обработки ПДн невозможно;

− выявления неправомерной обработки ПДн без согласия субъекта ПДн.

В случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного законом, Организация обеспечивает их блокирование с последующим обеспечением уничтожения ПДн. Уничтожение ПДн производится не позднее шести месяцев со дня их блокирования.

Б.6 В Организации определена, выполняется и контролируется политика в отношении обработки ПДн, а также установлен порядок обработки ПДн для отдельных ресурсов ПДн. Для ресурсов ПДн, обрабатываемых в АС, в том числе АС, порядок обработки ПДн может являться частью эксплуатационной документации на АС и разрабатываться на этапе создания (модернизации) АС.

Указанные документы:

− определяют процедуры предоставления доступа к ПДн;

− определяют процедуры внесения изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн;

− определяют процедуры уничтожения, обезличивания либо блокирования ПДн в случае необходимости выполнения таких процедур;

− определяют процедуры обработки обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом «О персональных данных», в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (их законных представителей) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки;

− определяют процедуры обработки запроса уполномоченного органа по защите прав субъектов ПДн;

− определяют процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу обработки его ПДн третьим лицам;

− определяют процедуры передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками Организации, имеющими доступ к ПДн;

− определяют процедуры передачи ПДн третьим лицам;

− определяют процедуры работы с материальными носителями ПДн;

− определяют процедуры, необходимые для осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные законом;

− определяют необходимость применения типовых форм документов для осуществления обработки ПДн и процедуры работы с ними. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая Организацией с целью сбора ПДн.

Б.7 Организация обеспечен неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, а также к сведениям о реализуемых требованиях по обеспечению безопасности персональных данных. Доступ к документу реализован путем размещения документа на официальном сайте ООО МКК «Экофинанс» по адресу: creditplus.ru.

Б.8 В Организации установлено, в каких случаях необходимо получение согласия субъектов ПДн, при этом регламентированы форма и порядок получения согласия субъектов ПДн.

Б.9 В Организации определен и выполняется учет лиц, имеющих доступ к ПДн.

Б.10 Обработка ПДн работниками Организации должны осуществляться только с целью выполнения их должностных обязанностей.

Б.11 В Организации определены, выполняться, регистрироваться и контролироваться процедуры ознакомления работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами Организации, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

Б.12 В Организации определены помещения, в которых осуществляется обработка ПДн.

Б.13 При работе с МНИ ПДн обеспечено выполнение содержания, предусмотренного мерами ПУИ.20, ПУИ.21, ПУИ.22, ПУИ.24, а также:

− обособление ПДн от иной информации, в частности путем фиксации их на отдельных МНИ ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);

− хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных МНИ;

− регистрация и учет мест хранения МНИ ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

− установление и выполнение порядка гарантированного уничтожения (стирания) информации с МНИ ПДн.

Б.14 Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

Б.15 Общедоступные источники ПДн создаются и публикуются Организацией только для цели выполнения требований законодательства Российской Федерации.

Б.16 Поручение обработки ПДн третьему лицу (далее - обработчик) осуществляется на основании договора. В указанном договоре определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн.

Б.17 В Организации определены и выполняются процедуры, выполняемые в случаях необходимости осуществления трансграничной передачи ПДн.

Б.18 В Организации назначено лицо, ответственное за организацию обработки ПДн.

РАЗДЕЛ 5.6. ОСНОВНЫЕ ПОЛОЖЕНИЯ БАЗОВОЙ МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

А.1 Основой для реализации Организацией системы защиты информации являются общепринятые модели угроз и нарушителей безопасности информации.

Степень детализации содержимого моделей угроз и нарушителей безопасности информации может быть различна и при необходимости определяется реальными потребностями Организации.

А.2 Модели угроз и нарушителей безопасности информации носят прогнозный характер и разрабатываются на основе опыта, знаний и практики Организации, с учетом того, что со временем угрозы, их источники и сопутствующие риски могут изменяться.

А.3 В случае отсутствия у Организации потенциала, необходимого для самостоятельной разработки моделей угроз и нарушителей безопасности информации, указанные модели могут быть определены с привлечением сторонних организаций, обладающих необходимым опытом, знаниями и компетенцией.

При разработке моделей угроз и нарушителей безопасности информации необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все критические операции в рамках бизнес-процессов и технологических процессов Организации, где осуществляется любое взаимодействие субъектов доступа с объектами информатизации, тщательно контролируются.

Организация признает, что наиболее уязвимым будет являться нарушение непрерывности предоставления финансовых услуг, осуществления бизнес-процессов или технологических процессов Организации, например, посредством распространения вредоносного кода, целенаправленных компьютерных атак или нарушения правил эксплуатации на уровне аппаратного обеспечения.

А.5 Основными типами источников угроз безопасности информации являются:

− неблагоприятные события техногенного характера;

− сбои и отказы в работе объектов и (или) ресурсов доступа;

− зависимость процессов эксплуатации объектов информатизации от иностранных поставщиков или провайдеров услуг;

− внутренние нарушители безопасности информации лица, в том числе работники Организации и работники подрядных организаций, реализующие угрозы безопасности информации с использованием легально предоставленных им прав логического или физического доступа;

− внешние нарушители безопасности информации лица, в том числе работники Организации, реализующие угрозы безопасности информации без использования легально предоставленных прав логического или физического доступа, а также субъекты, не являющиеся работниками Организации, реализующие целенаправленные компьютерные атаки, в том числе с целью личного обогащения или блокирования штатного функционирования бизнес-процессов или технологических процессов Организации.

А.6 К числу наиболее актуальных источников угроз на уровне аппаратного обеспечения, уровне сетевого оборудования и уровне сетевых приложений и сервисов относятся следующие:

− сбои и отказы в работе объектов доступа;

− внутренние нарушители безопасности информации [эксплуатационный, вспомогательный (технический) персонал], осуществляющие целенаправленное деструктивное воздействие на объекты доступа;

− зависимость процессов эксплуатации объектов доступа от иностранных поставщиков или провайдеров услуг;

− внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

− внешние нарушители безопасности информации, организующие DoS, DDoS и иные виды компьютерных атак;

− комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие совместно и (или) согласованно.

А.7 К числу наиболее актуальных источников угроз на уровне серверных компонентов виртуализации, программных инфраструктурных сервисов, операционных систем, систем управления базами данных и серверов приложений относятся следующие:

− внутренние нарушители безопасности информации (эксплуатационный персонал), осуществляющие целенаправленные деструктивные воздействия на ресурсы доступа;

− внутренние нарушители безопасности информации (эксплуатационный персонал), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;

− сбои и отказы в работе ПО;

− зависимость процессов эксплуатации ресурсов доступа, ПО от иностранных поставщиков или провайдеров услуг;

− внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

− комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

А.8 К числу наиболее актуальных источников угроз на уровне АС и приложений, эксплуатируемых в рамках бизнес-процессов и технологических процессов Организации, относятся следующие:

− внутренние нарушители безопасности информации (пользователи и эксплуатационный персонал АС и приложений), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;

− внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

− зависимость процессов эксплуатации АС и приложений от иностранных поставщиков или провайдеров услуг;

− комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

А.9 Наибольшими возможностями для нанесения ущерба Организации обладают ее собственные работники. В этом случае содержанием деятельности нарушителя является прямое нецелевое использование предоставленных прав физического и (или) логического доступа. При этом он будет стремиться к сокрытию следов своей деятельности.

РАЗДЕЛ 5.7. ПЕРЕЧЕНЬ СОБЫТИЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПОТЕНЦИАЛЬНО СВЯЗАННЫХ С НЕСАНКЦИОНИРОВАННЫМ ДОСТУПОМ И ИНЦИДЕНТАМИ ЗАЩИТЫ ИНФОРМАЦИИ, РЕКОМЕНДУЕМЫХ ДЛЯ ВЫЯВЛЕНИЯ, РЕГИСТРАЦИИ И АНАЛИЗА

В.1 Действия и (или) операции по созданию, удалению, копированию ресурсов доступа.

В.2 Действия и (или) операции по созданию, удалению, блокированию, разблокированию учетных записей.

В.3 Действия и (или) операции по изменению (предоставлению) прав логического доступа.

В.4 Действия и (или) операции по подключению СВТ к вычислительным сетям Организации.

В.5 Действия и (или) операции по запуску программных процессов.

В.6 Действия и (или) операции при осуществлении логического доступа.

В.7 Факты выявления уязвимостей защиты информации.

В.8 Факты выявления вредоносного кода и (или) мобильного кода.

В.9 Факты выявления попыток осуществления вторжений и сетевых атак.

В.10 Факты выявления атак типа «отказ в обслуживании».

В.11 Действия и (или) операции, направленные на изменение правил сегментации и межсетевого экранирования вычислительных сетей Организации.

В.12 Действия и (или) операции по изменению параметров настроек технических мер защиты информации, параметров настроек системного ПО, влияющих на обеспечение защиты информации.

В.13 Факты выявления нарушений и сбоев в работе технических мер защиты информации.

В.14 Факты выявления нарушений и сбоев в установлении (обновлении) ПО и параметров настроек технических мер защиты информации, их сигнатурных баз (в случае их использования).

В.15 Факты выявления нарушений и сбоев в установлении (обновлении) системного ПО и параметров его настроек, влияющих на обеспечение защиты информации.

В.16 Действия и (или) операции по изменению состава ПО АРМ пользователей и эксплуатационного персонала, в том числе запускаемого автоматически при загрузке операционных систем.

В.17 Действия и (или) операции по изменению состава ПО серверного оборудования.

В.18 Факты выявления нарушений целостности ПО АС на АРМ пользователей и эксплуатационного персонала.

В.19 Факты выявления нарушений доверенной загрузки операционных систем АРМ пользователей и эксплуатационного персонала.

В.20 Факты выявления нарушений целостности эталонных копий ПО, в том числе при осуществлении их распространения и (или) обновления.

В.21 Факты выявления смены и (или) компрометации аутентификационных данных, используемых для доступа к серверному и сетевому оборудованию.

В.22 Действия и (или) операции со средствами криптографической защиты информации и ключевой информацией.

В.23 Действия и (или) операции по использованию разблокированных коммуникационных портов.

В.24 Действия и (или) операции по передаче информации с использованием электронной почты.

В.25 Действия и (или) операции при осуществлении доступа к ресурсам сети Интернет.

В.26 Действия и (или) операции при осуществлении доступа к серверным компонентам виртуализации виртуальными машинами, логическими разделами или томами.

В.27 Факты выявления нарушений при доверенной загрузке виртуальных машин.

В.28 Действия и (или) операции при администрировании системы хранения данных.

В.29 Действия и (или) операции по использованию подконтрольных мобильных устройств.

ГЛАВА 6. СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

РАЗДЕЛ 6.1. ПЕРЕЧЕНЬ БИЗНЕС-ПРОЦЕССОВ, ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И АС ОРГАНИЗАЦИИ

6.1.1. Описание бизнес-процессов Организации приведено в Таблице 1.

Таблица 1

Наименование процессов	Описание процесса
Процесс 1	осуществление расчетных операций

Процесс 2	выдача и погашение займов
Процесс 3	пассивные операции (привлечение вкладов, получение кредитов в банках, иные операции)
Процесс 4	оформление трудовых отношений с работниками Организации, обработка персональных данных работников Организации
Процесс 5	обмен информацией с Банком России, ФНС, иными государственными регуляторами и Организациями
Процесс 6	обработка персональных данных клиентов Организации

6.1.3. Состав установленного и используемого в АС программного обеспечения соответствует определенному перечню. Выполнение данных требований контролируется системным администратором (СА) с документированием результатов.

6.1.4. Порядок обмена платежной информацией зафиксирован в договорах между участниками, осуществляющими обмен платежной информацией.

6.1.5. Работники Организации, в том числе администраторы АС и средств защиты информации, не обладают полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций.

6.1.6. Результаты технологических операций по обработке информации должны контролироваться (проверяться) и удостоверяться лицами/автоматизированными процессами.

6.1.7. Обязанности по администрированию средств защиты информации возложены на СА с отражением этих обязанностей в их должностных инструкциях.

Порядок администрирования средств ИБ в Организации изложен в Приложении № 5 к настоящей Политике.

6.1.7. Комплекс мер по обеспечению ИБ Процессов 1-3,5 включает в том числе:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;
- доступ работника Организации только к тем ресурсам технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию входящих электронных платежных сообщений;
- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
- возможность ввода информации в АС только для авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

Кроме того, Организации при появлении угроз защите информации может быть организован авторизованный ввод информации в АС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип «двойного управления»).

6.1.8. Комплекс мер по обеспечению ИБ Процесса 6 включает:

- защиту информации от искажения, фальсификации, переадресации, несанкционированной отправки третьим лицам;
- доступ работника Организации только к тем ресурсам технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения персональных данных;
- аутентификацию входящих документов, содержащих персональные данные;
- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена;
- возможность ввода информации в АС только для авторизованных пользователей;
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- доставку электронных сообщений участникам обмена.

6.1.9. При проектировании, разработке и эксплуатации систем дистанционного взаимодействия планируется документально определить и выполнят процедуры, реализующие в том числе механизмы:

- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными пользователями;
- доведения информации о возможных рисках, связанных с выполнением операций или транзакций до пользователей.

Пользователей систем дистанционного обслуживания планируется обеспечивать детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

6.1.10. Процедуры обслуживания программных средств вычислительной техники, используемых в технологическом процессе, включая замену их программных и (или) аппаратных частей, определены договорными обязательствами поставщиков (исполнителями). Все изменения в программные средства определяются в соответствии с изменениями законодательства РФ и нормативных правовых актов Банка России.

Процедуры обслуживания аппаратных частей вычислительной техники, используемых в технологическом процессе, определены договорными обязательствами поставщиков (исполнителями), сроками амортизации и моральной изношенностью технических средств.

Программно-аппаратные средства обеспечивают возможность отслеживания состояния АС в целом и в части применения к отдельным процессам.

Все перебои в работе систем сигнализируются. Контроль осуществляется дублирующим способом.

В случае назначения ответственного за ИБ Организации лица, ответственное за ИБ лицо производит самостоятельный контроль обеспечения информационной безопасности информации.

6.1.12. В Организации реализована процедура оперативного восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ информации при любых сбоях работы системы. Восстановление осуществляется СА Организации.

В случае возникновения ситуации требующей внимания, СА должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуации и принятых мерах необходимо ставить в известность СА.

В случае возникновения угрожающей или серьезной критической ситуации действия работников включают следующие этапы:

- немедленная реакция;
- частичное восстановление работоспособности и возобновление обработки;
- полное восстановление системы и возобновление обработки в полном объеме;
- расследование причин кризисной ситуации и установление виновных.

Этапы включают следующие действия:

В качестве немедленной реакции:

- обнаруживший факт возникновения кризисной ситуации работник ООО МКК «Экофинанс» обязан немедленно оповестить об этом СА;
- СА должен поставить в известность работников - пользователей всех смежных систем о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- вызвать СА;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.
- Ответственным за этот этап является СА.

При частичном восстановлении работоспособности (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) и возобновлении обработки:

- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих систем.
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить поврежденное критичное программное обеспечение, используя эталонные (страховые) копии;

- восстановить необходимые данные, используя страховые копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить работников - пользователей смежных систем о готовности к работе.
- Затем необходимо внести все изменения данных за время с момента создания последней страховой копии (за текущий период, операционный день), для чего должен осуществляться «докат» на основании информации из журналов транзакций либо все связанные с поврежденной системой пользователи должны повторить действия выполненные в течение последнего периода (дня).

Ответственным за этот этап является СА.

Для полного восстановления в период неактивности системы:

- восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;
- восстановить все поврежденные данные, используя страховые копии и журналы транзакций;
- настроить средства защиты подсистемы в соответствии с планом защиты;
- о результатах восстановления уведомить администратора системы (базы данных), назначенного приказом по Организации.

Ответственным за этот этап является СА.

Далее необходимо провести расследование причин возникновения кризисной ситуации. Для этого необходимо ответить на вопросы:

- случайная или преднамеренная кризисная ситуация?
- можно ли было ее предусмотреть?
- вызвана ли она слабостью средств защиты и регистрации?
- превысил ли ущерб от нее установленный уровень?
- есть ли невосполнимый ущерб и велик ли он?
- это первая кризисная ситуация такого рода?
- есть ли возможность точно определить круг подозреваемых?
- есть ли возможность точно установить виновника?
- в чем причина кризисной ситуации?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра плана защиты?
- есть ли необходимость пересмотра плана обеспечения непрерывной работы и восстановления?

Ответственным за расследование является СА. Отчет о результатах расследования и предложениях по совершенствованию системы должен быть направлен руководству.

6.1.11. Описание иных хозяйственных процессов

Не входящие в состав данных АС серверы, офисные ЭВМ и другое оборудование должно быть изолировано от АС на уровне локальных вычислительных сетей способом, согласованным с СА либо лицом, отвечающим за ИБ.

6.1.12. В информационном технологическом процессе используется программное обеспечение, сертифицированное и распространяемое в соответствии с требованиями законодательства и необходимого для реализации конкретных информационных технологических процессов. Перечень программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АС и необходимого для выполнения конкретных информационных технологических процессов, приведен в Таблице 3.

Состав установленного и используемого в ЭВМ и АС программного обеспечения может расширяться в зависимости от текущих задач, и соответствует условиям договорных обязательствах поставщиков (исполнителей) и требованиям, указанных в технической документацией на АС.

Состав установленного и используемого в ЭВМ и АС программного обеспечения соответствует определенному перечню. Выполнение данных требований контролируется, с документированием результатов при случаях нарушениях и сбоев в работе программного обеспечения .

6.1.13. В Организации должна осуществляться ежедневная процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ неплатежной информации по следующим направлениям:

- сопровождение программно-технических средств (ПТС), включая вопросы организации работы и контроля за использованием ПТС в АС;

- оперативный контроль за функционированием ПТС;
- контроль соответствия общесистемной программной среды эталону.

Программно-аппаратные средства обеспечивают возможность отслеживания СА состояния АС в целом и в части применения к отдельным платежным процессам.

Все перебои в работе систем сигнализируются СА и администратору ИБ или иному уполномоченному лицу. Контроль осуществляется дублирующим способом.

6.1.14. В Организации осуществляется процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ неплатежной информации. Регламентирующие документы должны быть согласованы с СА.

Восстановление осуществляется СА.

В случае возникновения ситуации требующей внимания, СА должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуации и принятых мерах необходимо ставить в известность СА.

В случае возникновения угрожающей или серьезной критической ситуации действия работников включают следующие этапы:

- немедленная реакция;
- частичное восстановление работоспособности и возобновление обработки;
- полное восстановление системы и возобновление обработки в полном объеме;
- расследование причин кризисной ситуации и установление виновных.

Этап включают следующие действия:

в качестве немедленной реакции:

- обнаруживший факт возникновения кризисной ситуации работник обязан немедленно оповестить об этом СА;
- СА должен поставить в известность работников - пользователей всех смежных систем о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- вызвать СА;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.
- Ответственным за этот этап является СА.
- При частичном восстановлении работоспособности (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) и возобновлении обработки:
- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих систем.
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить поврежденное критичное программное обеспечение, используя эталонные (страховые) копии;
- восстановить необходимые данные, используя страховые копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить работников - пользователей смежных систем о готовности к работе.
- Затем необходимо внести все изменения данных за время с момента создания последней страховой копии (за текущий период, операционный день), для чего должен осуществляться «докат» на основании информации из журналов транзакций либо все связанные с поврежденной системой пользователи должны повторить действия выполненные в течение последнего периода (дня).

Ответственным за этот этап является СА.

Для полного восстановления в период неактивности системы:

- восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;

− восстановить все поврежденные данные, используя страховые копии и журналы транзакций;
− настроить средства защиты подсистемы в соответствии с планом защиты;
− о результатах восстановления уведомить администратора системы (базы данных), назначенного приказом по Организации.
− Ответственным за этот этап является СА.
− Далее необходимо провести расследование причин возникновения кризисной ситуации. Для этого необходимо ответить на вопросы:
− случайная или преднамеренная кризисная ситуация?
− можно ли было ее предусмотреть?
− вызвана ли она слабостью средств защиты и регистрации?
− превысил ли ущерб от нее установленный уровень?
− есть ли невосполнимый ущерб и велик ли он?
− это первая кризисная ситуация такого рода?
− есть ли возможность точно определить круг подозреваемых?
− есть ли возможность точно установить виновника?
− в чем причина кризисной ситуации?
− достаточно ли имеющегося резерва?
− есть ли необходимость пересмотра плана защиты?
− есть ли необходимость пересмотра плана обеспечения непрерывной работы и восстановления?

Ответственным за расследование является СА. Отчет о результатах расследования и предложениях по совершенствованию системы необходимо направить руководству.

РАЗДЕЛ 6.2. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБРАБОТКЕ В ОРГАНИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования по обработке персональных данных регламентируются Политикой в отношении обработки и защиты персональных данных ООО МКК «Экофинанс», разработанной в соответствии с требованиями Федерального закона «О персональных данных».

6.2.1. Для каждой цели обработки персональных данных определены, документально зафиксированы и утверждены руководством :
− объем и содержание персональных данных;
− сроки обработки, в том числе сроки хранения персональных данных;
− необходимость получения согласия субъектов персональных данных.

6.2.2. Передача персональных данных третьему лицу осуществляется с согласия субъекта персональных данных. В том случае, если Организация поручает обработку персональных данных третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

6.2.3. Организация прекращает обработку персональных данных и уничтожает собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:
− по достижении целей обработки или при утрате необходимости в их достижении;
− по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
− при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
− при невозможности устранения работником ООО МКК «Экофинанс» допущенных нарушений при обработке персональных данных.

Уничтожения персональных данных (в том числе и материальных носителей персональных данных) производится в следующем порядке:

уничтожение персональных данных субъекта осуществляется комиссией либо уполномоченным работником, созданной (уполномоченным) на основании приказа руководителя Организации. Документально уничтожение персональных данных субъекта оформляется соответствующим актом о прекращении обработки персональных данных.

6.2.4. В Организации определен и документально зафиксирован порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных.

6.2.5. В Организации определен порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

6.2.6. Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения информационного технологического процесса, реализацию которого поддерживает АС, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

6.2.7. Информационные технологические процессы, в рамках которых обрабатываются персональные данные в АС, документированы.

При этом исключена фиксация на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы.

При обработке различных категорий персональных данных используется отдельный материальный носитель.

6.2.8. В Организации определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в АС либо имеющих доступ к персональным данным.

Допускается указание работников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью на основании требований соответствующего стандарта Банка России.

Возможно существование перечня (списка) в электронном виде при условии предоставления работникам прав доступа в АС только на основании распорядительного документа в документально зафиксированном в Организации порядке.

Доступ работников к персональным данным и обработка персональных данных работниками должны осуществляться только для выполнения их должностных обязанностей.

6.2.9. Работники, осуществляющие обработку персональных данных в АС, должны быть проинформированы о факте обработки ими персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

6.2.10. В Организации должен быть определен порядок доступа работников и иных лиц в помещения, в которых ведется обработка персональных данных.

6.2.11. В Организации определен порядок хранения материальных носителей персональных данных.

6.2.13. При обработке в Организации персональных данных на бумажных носителях, в частности, при использовании в Организации типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные законодательно в области обработки персональных данных, осуществляемой без использования средств автоматизации.

РАЗДЕЛ 6.3. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ, В РАМКАХ КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Порядок использования средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным, регламентирован в Организации Политикой в отношении обработки и защиты персональных данных ООО МКК «Экофинанс».

6.3.1. СИБ технологического процесса и СИБ информационного технологического процесса, в рамках которого обрабатываются персональные данные, должны соответствовать требованиям Банка России.

6.3.2. Все АС, в которых происходит обработка персональных данных, относятся к

специальным в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

6.3.3. Требования по обеспечению безопасности персональных данных при их обработке в АС определяются на основе Стандартов Банка России. Актуальными являются те угрозы, риск реализации которых в Организации является недопустимым.

Результатом оценки рисков нарушения безопасности персональных данных является Модель угроз безопасности персональных данных, содержащая актуальные для угрозы ИБ, на основе которой вырабатываются требования, учитывающие особенности обработки персональных данных в Организации.

РАЗДЕЛ 6.4. ПЕРЕЧЕНЬ ТИПОВ ИНФОРМАЦИОННЫХ АКТИВОВ В ОРГАНИЗАЦИИ

6.4.1. Вся обрабатываемая Организацией информация подразделяется на типы:

- информация ограниченного доступа;
- информация, содержащая сведения, составляющие тайну об операциях клиентов;
- платежная информация (информация, предназначенная для проведения расчетных, и других операций и учетных операций);
- информация, содержащая сведения, составляющие коммерческую тайну;
- персональные данные;
- управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации);
- открытая (общедоступная) информация.

6.4.2. Классификация информационных активов проведена на основании оценок ценности информационных активов для интересов (целей) в соответствии с тяжестью последствий потери свойств ИБ информационных активов.

Таблица 5

вид информационного актива	перечень составляющих	Свойства информационной безопасности конфиденциальность целостность доступность
информация ограниченного доступа; информация, содержащая сведения, составляющие тайну об операциях клиентов;	персональные данные (выделенный актив); сведения о клиентах, о состоянии счетов, производимых операциях, сведения составляющие тайну;	потеря свойств ИБ влечет административную и уголовную ответственность, тяжелые последствия для Организации потеря свойств ИБ влечет ответственность в виде возмещения причиненных убытков, тяжелые последствия для ограничиваются материальной компенсацией убытков пострадавшего лица
платежная информация (информация, предназначенная для проведения расчетных, и других платежных операций и учетных операций);	сведения о хозяйственных операциях;	потеря свойств ИБ влечет разглашение коммерческой тайны, последствия зависят от свойств информации, влекут потерю конкурентоспособности
информация, содержащая сведения, составляющие коммерческую тайну;	информация о третьих лицах, полученная в ходе осуществления хозяйственной деятельности;	потеря свойств ИБ влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, последствия могут оказаться тяжелыми для

		Организации
персональные данные;	информация, полученная у работников с целью оформления трудовых отношений	если потеря свойств ИБ не повлечет раскрытие информации о персональных данных, последствия минимальны
управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации); открытая (общедоступная) информация	сведения о клиентах, о состоянии счетов, производимых операциях, сведения составляющие коммерческую тайну, тайну об операциях клиентов, сведения о защитных средствах;	потеря свойств ИБ влечет ответственность в виде возмещения причиненных убытков, тяжелые последствия для не ограничиваются материальной компенсацией убытков пострадавшего лица, а влечет хозяйственные потери и риск возмещения убытков третьим лицам
носители информации	бумажные	потеря свойств ИБ имеет последствия, зависящие от информационного состава информации на этих носителях
	электронные (все виды электронных носителей)	потеря свойств ИБ имеет последствия, зависящие от информационного состава информации на этих носителях
программное и аппаратное обеспечение	(указано выше)	в Организации используется массово тиражируемое программное обеспечение. Потеря свойств ИБ повлечет только те последствия, которые связаны с характером обрабатываемых таким обеспечением информации

6.4.3. Опись информационных активов содержит информацию о принадлежности информационного актива к выделенным типам информационных активов ввиду его особой охраняемости в соответствии с требованиями законодательства.

6.4.4. Перечень объектов среды информационных активов покрывает все уровни информационной инфраструктуры Организации

РАЗДЕЛ 6.5. ПЕРЕЧЕНЬ ТИПОВ ОБЪЕКТОВ СРЕДЫ ИЕРАРХИЯ ИНФОРМАЦИОННЫХ АКТИВОВ ОРГАНИЗАЦИИ

6.5.1. В организации используются следующие объекты информационной среды:

- линии связи и сети передачи данных;
- сетевые программные и аппаратные средства, в том числе сетевые серверы;
- файлы данных, базы данных, хранилища данных;
- прикладные и общесистемные программные средства;
- программно-технические компоненты автоматизированных систем;
- помещения, здания;
- платежные и информационные технологические процессы.

По степени конфиденциальности информационные ресурсы Организации подразделяются на типы:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Организации;
- открыто распространяемая информация, необходимая для работы Организации, независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы

информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Тип информационного актива	Уровни иерархии информационной инфраструктуры	Типы объектов среды
линии связи и сети передачи данных; сетевые программные и аппаратные средства, в том числе сетевые серверы; файлы данных, базы данных, хранилища данных; прикладные и общесистемные программные средства; программно-технические компоненты автоматизированных систем; помещения, здания, сооружения; платежные и информационные технологические процессы	Физический уровень	Линии связи, аппаратные и технические средства, физические носители информации
	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы
	Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)

Применяемые Организацией меры защиты информации обеспечивают контроль:

- области применения процесса системы защиты информации;
- должного применения мер защиты информации в рамках процесса системы защиты информации;
- знаний работников Организации в части применения мер защиты информации.
- политику обеспечения защиты информации Организации;
- область применения системы защиты информации, описанной как перечень бизнес-процессов, технологических процессов и (или) АС Организации;
- целевые показатели величины допустимого остаточного операционного риска, связанного с нарушением безопасности информации;
- положения о выделении необходимых и достаточных ресурсов, используемых при применении организационных и технических мер, входящих в систему защиты информации.

РАЗДЕЛ 6.6. ПРОЦЕДУРЫ АНАЛИЗА И ПЕРЕСМОТРА ОБЛАСТИ ДЕЙСТВИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ:

6.6.1. СА периодически проводит анализ функционирования системы информационной безопасности организации (СОИБ). Данный анализ основывается на следующих данных:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри;
- данные об изменениях вне Организации.

6.6.2. Анализ функционирования СОИБ включает в себя также:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в Организации, требованиям законодательства Российской Федерации, требованиям стандартов Банка России;

- оценку рисков в области ИБ;
- проверку адекватности используемых защитных мер требованиям внутренних документов и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

6.6.3. В случае выявления необходимости пересмотра области действия СОИБ, в частности, пересмотра при изменении перечня информационных активов (типов информационных активов), СА производит корректирующие действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ и не требующих пересмотра политик ИБ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа «планирование».

6.6.4. Для принятия решений, связанных с тактическими улучшениями СОИБ, рассматриваются документально оформленные результаты:

- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- стратегических улучшений СОИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

6.6.5. К стратегическим улучшениям СОИБ относятся корректирующие действия, связанные с пересмотром политики ИБ организации, с последующим выполнением соответствующих тактических улучшений СОИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа «планирование».

Для принятия решений, связанных со стратегическими улучшениями СОИБ, рассматриваются документально оформленные результаты:

- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций),
- а также изменения:
- в законодательстве Российской Федерации;
- в нормативных актах Банка России;
- интересов, целей и задач.

Обязанность по определению/коррекции области действия СОИБ в Организации, по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ, возложена на СА. Ответственным за выполнение указанных действий является СА.

РАЗДЕЛ 6.7. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

6.7.1. Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Организации функции обеспечения ИБ возложены на СА. На это подразделение возлагается решение следующих основных задач:

- проведение в жизнь Политики ИБ;
- определение требований к защите информации;
- Организации мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;

− оказание методической помощи работникам в вопросах обеспечения информационной безопасности;

− регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;

− выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения;

− обеспечение минимально необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;

− информирование, обучение и повышение квалификации работников Организации в сфере информационной безопасности;

− расследования инцидентов информационной безопасности;

− сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;

− обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

6.7.2. Для решения задач, возложенных на СА, его работники имеют следующие права:

− определять необходимость и разрабатывать локальные правовые акты, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;

− получать информацию от пользователей информационных систем Организации по любым аспектам применения информационных технологий в Организации;

− участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;

− участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;

− контролировать деятельность пользователей по вопросам обеспечения ИБ;

− готовить предложения руководству по обеспечению требований ИБ.

6.7.3. В Организации определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями Организации. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

− учесть изменения бизнес-требований и приоритетов;

− принять во внимание новые угрозы и уязвимости;

− убедиться в том, что реализованные средства сохранили свою эффективность.

6.7.4. Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ, должны быть доведены до работника, в чьи обязанности будет входить работа с информационными ресурсами, при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

6.7.5. Все принимаемые на работу работники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие работника на проведение контрольных мероприятий со стороны Организации по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения работником требований ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого работника Организации.

Все принимаемые работники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении работнику доступа к ИС Организации он должен ознакомиться под роспись с инструкцией пользователя ИС или с инструкцией пользователя ИС.

6.7.9. Руководство Организации должно требовать от всех работников, подрядчиков и

пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Организации политиками и процедурами.

Уполномоченные руководством Организации работники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования работниками информационных ресурсов;
- Содержания служебной переписки.

6.7.10. Все работники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Организации.

6.7.11. При увольнении все предоставленные работнику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

6.7.12. Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Организации, должны быть размещены в защищённых областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

6.7.13. Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Запрещается приём посетителей в помещениях, когда осуществляется обработка информации ограниченного доступа.

6.7.14. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком.

6.7.15. Места доступа, через которые неавторизованные лица могут попасть в помещения Организации, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

6.7.16. Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Организации.

6.7.17. Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, гарантированно удаляются все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях проверяется СА Организации, о чём должна быть сделана отметка в акте списания.

6.7.18. Оборудование, информация или ПО должны перемещаться за пределы Организации только при наличии письменного разрешения руководства. Работники, имеющие право перемещать оборудование и носители информации за пределы Организации определены внутренними документами Организации. Время перемещения оборудования за пределы Организации и время его возврата должны регистрироваться.

6.7.19. Основными пользователями информации в информационной системе Организации являются работники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый работник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами строго регламентирован. Любые изменения состава и полномочий пользователей подсистем производятся в установленном порядке.

Каждому пользователю, допущенному к работе с конкретным информационным активом Организации, сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИА.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, работникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Регистрируемые учётные записи подразделяются на:

− Пользовательские предназначенные для аутентификации пользователей ИР Организации;

− Системные используемые для нужд операционной системы;

− Служебные предназначенные для функционирования отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и используются только в случаях, предписанных документацией на операционную систему.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

− использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;

−

− предоставление и блокирование прав должны быть санкционированы и документированы;

− предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;

− регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Организации;

− уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;

− согласование изменения прав доступа с СА;

− документальная фиксация назначенных пользователю прав доступа;

− предоставление доступа с момента завершения процедуры регистрации;

− обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;

− немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Организации;

− аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;

−

− обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

6.7.20. Доступ работника к информационным ресурсам Организации должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный работник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование является строго ограниченным и управляемым.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Организации осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

6.7.21. Пароли - средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

− все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;

− при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;

− временные пароли должны назначаться пользователю только после его идентификации;

− необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;

− временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;

− пользователь должен подтвердить получение пароля;

− пароли должны храниться в электронном виде только в защищенной форме;

− назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;

− необходимо установить требования к длине пароля, набору символов и числу попыток ввода;

− необходимо изменять пароля пользователя, в соответствии с внутренними требованиями.

−

6.7.22. Чтобы обеспечить эффективный контроль доступа Организация вправе ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

− права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;

− права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Организации, а также при переходе с одной работы на другую в пределах организации;

− проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);

− необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

− изменение привилегированных учетных записей должно протоколироваться.

− контроль над выполнением процедур управления доступом пользователей должен включать:

− контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;

− проверку подлинности пользователей перед сменой паролей;

− немедленное блокирование прав доступа при увольнении;

− блокирование учётных записей, неактивных более 45 дней;

− устройства в течение не менее трёх лет;

− ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;

− использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;

− разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;

− блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;

− блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены СА к событиям нарушения безопасности информации.

6.7.23. Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых работнику Организации предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) работником информации.

Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает СА либо иное уполномоченное лицо. Личные пароли первоначально устанавливает СА. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

− длина пароля должна быть не менее 8 символов;

− в числе символов пароля должны присутствовать три из четырёх видов символов:

буквы в верхнем регистре;

буквы в нижнем регистре;

цифры;

специальные символы (! @ # $ % ^ & * ( ) _ + = ~ [ ] { } | \ :; ООО МКК “Экофинанс” « < >,. ? /);

− пароль не должен содержать легко вычисляемые сочетания символов, например, имена, фамилии, номера телефонов, даты;

последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);

− при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;

Работнику рекомендуется выбирать пароль с помощью следующей процедуры:

− выбрать фразу, которую легко запомнить. Например, «Три мудреца в одном тазу пустились по морю в грозу»;

− Выбрать первые буквы из каждого слова «тмвотппмвг»;

− Набрать полученную последовательность, переключившись на английскую раскладку клавиатуры: «nvdjnggvdu»;

− Выбрать номер символа, который будет записываться в верхнем регистре и после которого будет специальный символ. Например, это будет пятый символ, а в качестве специального символа выбран «#». Получаем: «nvdjN#ggvdu».

Работнику запрещается:

− сообщать свой пароль кому-либо;

− указывать пароль в сообщениях электронной почты;

− хранить пароли, записанные на бумаге, в легко доступном месте;

− использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

− использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Сотрудник обязан:

− в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации СА;

− немедленно сообщить СА в случае получения от кого-либо просьбы сообщить пароль;

− менять пароль в соответствии с внутренними требованиями;

− менять пароль по требованию Администратора ИБ.

Организация оставляет за собой право:

− осуществлять периодическую проверку стойкости паролей пользователей, используемых работниками для доступа к ИС;

− принимать меры дисциплинарного характера к работникам, нарушающим положения настоящей политики.

6.7.25. Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

6.7.26. Работники Организации обязаны:

− сохранять известные им пароли в тайне;

− закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;

− по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён в Организации в установленном порядке.

Документы и носители с конфиденциальной информацией должны убираться в специально отведенные места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из

системы, когда они находятся без присмотра.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня работник должен привести в порядок письменный стол и убрать все офисные документы в специальный шкаф или сейф.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

6.7.27. При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Организации. Необходимо учитывать риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищённой среде.

6.7.28. Общие обязанности пользователя:

− при работе с ПО руководствоваться нормативной документацией (руководством пользователя);

− обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

− знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;

− минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Организации.

6.7.29. На АРМ Организации допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках АРМ информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся у СА.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ. Указанные работы, а так же работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только СА.

6.7.30. К работе в ИС Организации допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Каждому работнику Организации, которому необходим доступ к ИР в рамках его должностных обязанностей, выдаются необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Организации, возложена на СА.

Каждый работник Организации, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

Работа в ИС работникам разрешена только на закреплённых за ними АРМ, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами.

Все АРМ, установленные в Организации, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Организации. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с СА. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется СА.

Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только СА.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к СА.

СА имеет право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

Передача документов внутри Организации производится только посредством общих папок, а также средствами электронной почты.

При работе в ИС Организации работник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Организации;
- использовать ИС и АРМ Организации исключительно для выполнения своих служебных обязанностей;
- ставить в известность СА о любых фактах нарушения требований ИБ;
- ставить в известность СА о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания СА Организации.
- Предоставлять АРМ СА для контроля;
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- в случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом СА.

При использовании ИС Организации запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:

конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с СА;

информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;

угрожающую, клеветническую, непристойную информацию;

- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Организации;
- предоставлять работникам Организации (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в разрешенное к использованию ПО;
- защищать информацию, способами, не согласованными с СА заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Организации;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС в случае нарушений протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Организации.

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Организации подлежат обязательной проверке на отсутствие вредоносного ПО.

6.7.31. Для выполнения своих служебных обязанностей каждый работник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Организации, базы данных, электронная почта.

Основными рабочими каталогами являются личные каталоги работников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ работников к ресурсам сети осуществляется согласно матрицы доступа. Временное расширение прав доступа осуществляется СА Организации в соответствии с действующим порядком предоставления (изменения) полномочий

пользователя.

6.7.32. При обработке конфиденциальной информации работники обязаны:

− знать и выполнять требования Инструкции по работе с конфиденциальной информацией;

− при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Организации применять средства защиты от неавторизованного доступа;

− размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;

− не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;

− обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;

− не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;

− не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;

− не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD диски, Flash устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

6.7.33. Электронная почта используется для обмена в рамках ИС Организации и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Организации пользователь должен учитывать:

− электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

− электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Организации необходимо осуществлять только в зашифрованном виде);

− электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Организации занимается СА.

Каждый работник Организации получает почтовый адрес в домене Организации. Адрес электронной почты выдаётся СА при начальной регистрации пользователя в домене Организации.

Корпоративная электронная почта Организации предназначена исключительно для использования в служебных целях.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Организации. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Организации и являются неотъемлемой частью его производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Организации либо удалены уполномоченными работниками Организации.

Пользователям корпоративной электронной почты Организации запрещено вести частную переписку с использованием средств корпоративной электронной почты Организации. К частной переписке относится переписка, не связанная с исполнением работником своих должностных обязанностей.

Использование корпоративной электронной почты Организации для частной переписки работником, является нарушением трудовой дисциплины Организации.

Каждый работник Организации имеет право на просмотр либо иное использование в интересах Организации сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты осуществляется уполномоченными работниками Организации в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Организации. Просмотр и иное

использование сообщений электронной почты в интересах Организации осуществляется работниками Организации в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса Организации работникам или группам работников, а также по мотивированным запросам прямых или непосредственных руководителей любых работников, чью почту необходимо использовать в интересах Организации.

Использование сообщений корпоративной электронной почты в интересах Организации, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения работников Организации должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

Формат подписи отправителя:
С уважением,
<Фамилия имя>
<Должность>
<Структурное подразделение>
<Наименование Организации>
<Адрес>
<номера контактов: телефон, мессенджеры, адреса электронной почты>
<сайт>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с СА.

Отказ от дальнейшего предоставления работнику Организации услуг электронной почты может быть вызван нарушениями требований настоящей политики.

Прекращение предоставления работнику Организации услуг электронной почты наступает при прекращении действия трудового договора (контракта) работника.

6.7.34. Доступ к сети Интернет предоставляется работникам Организации в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа работников Организации к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность СА о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

- использовать предоставленный Организацией доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Организации;
- Публиковать, загружать и распространять материалы содержащие:
  - Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с СА;
  - угрожающую, клеветническую, непристойную информацию;
  - вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;

— фальсифицировать свой IP адрес, а также прочую служебную информацию.

Организация оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Информация о посещаемых работниками Организации Интернет ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Организации для контроля.

Содержание Интернет ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

6.7.35. Под использованием мобильных устройств и носителей информации в ИС Организации понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.

На предоставленных Организацией мобильных устройствах допускается использование ПО, разрешённого к использованию ПО.

К предоставленным Организацией мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется СА. При использовании предоставленных Организацией мобильных устройств и носителей информации, работник обязан:

- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать СА о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных работнику Организации мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём/передача информации) инициированное работником Организации между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Организация оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации;

Информация об использовании работниками Организации мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также руководству Организации.

Информация, хранящаяся на предоставляемых Организацией мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.

6.7.36. СА регулярно проверяет сетевые ресурсы Организации антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) работник Организации должен незамедлительно оповестить об этом СА. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов работники подразделений обязаны:

- приостановить работу;

− немедленно поставить в известность о факте обнаружения заражения своего руководителя и СА, а также владельца файла и смежные подразделения, использующие эти файлы в работе.

− Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Для предупреждения вирусного заражения рекомендуется:

− никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

− удалять спам, рекламу и другие бесполезные сообщения;

− никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

− периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

6.7.37. При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Организации в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

6.7.38. Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

6.7.41. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом.

ЭЦП могут быть простыми (код, пароль).

Необходимо с особой тщательностью обеспечивать конфиденциальность ЭЦП, которую следует хранить в секрете, так как любой, имеющий к ней доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа.

Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

6.7.43. Чтобы свести к минимуму риск повреждения ИС, в Организации обеспечен контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объёмы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы всё же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

6.7.44. Чтобы свести к минимуму вероятность повреждения ИС Организации, следует ввести строгий контроль над внесением изменений. Программисты и иные СА, занимающиеся поддержкой, получают доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС критичные для бизнес-процессов Организации приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Организации.

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

РАЗДЕЛ 6.8. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.8.1. В Организации действует формальная процедура уведомления о происшествиях в

области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Организации при обращении с инцидентами.

В случае появления нарушений и сбоев, должны быть разработаны механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

6.8.2. При необходимости должен быть разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов Организации. Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнес-процессов.

В Организации должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов.

Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

6.8.3. Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Организации к обеспечению соответствия этим требованиям определены, документированы и поддерживаются в актуальном состоянии.

Персональные данные конкретного работника и процесс их обработки является открытым для этого работника.

В Организации внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Организации защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

Система хранения и обработки обеспечивает чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система имеет возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Организации.

6.8.4. Организация проводит внутренние проверки СУИБ через запланированные интервалы времени – то есть ежедневно, в штатном режиме.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

РАЗДЕЛ 6.9. ПРЕДОСТАВЛЕНИЕ УСЛУГ СТОРОННИМ ОРГАНИЗАЦИЯМ

6.9.1. В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

6.9.2. Услуги, отчёты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациямотчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

6.9.2. В Организации действует порядок приёмки новых ИС, обновления и новых версий ПО.

РАЗДЕЛ 6.10. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ ОРГАНИЗАЦИИ

Руководитель Организации определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, а также осуществляет общее руководство обеспечением ИБ Организации.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Организации лежит на СА или ином уполномоченном лице.

Все руководители подразделений Организации несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

Работники Организации несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности СА.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения обязанностей.

Руководство Организации регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов Организации по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

РАЗДЕЛ 6.11. КОНТРОЛЬ И ПЕРЕСМОТР ПОЛИТИКИ

6.11.1. Общий контроль состояния ИБ Организации осуществляется Руководителем.

Текущий контроль соблюдения настоящей Политики осуществляет СА или иное уполномоченное лицо. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Организации, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Изменения и дополнения вносятся по инициативе СА или иного уполномоченного лица и утверждаются Руководителем Организации.

ГЛАВА 7. ОСНОВНЫЕ ПОЛОЖЕНИЯ МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

Для разных бизнес-процессов Организации, составляющие различные контуры безопасности, в Организации разработаны типовые модели угроз.

Типовые модели Организации разработаны на основе анализа практики организации и носит прогнозный характер. Чем точнее сделан прогноз в отношении актуальных для Организации угроз безопасности информации, тем адекватнее и эффективнее будут планируемые и предпринимаемые усилия по обеспечению требуемого уровня защиты информации.

При этом, по мере изменения обстоятельств и технологий источники угроз и сопутствующие риски изменяются, поэтому типовая модель подлежит пересмотру, для чего СА должен ежедневно выполнять процедуры анализа результатов мониторинга угроз.

В случае отсутствия у СА потенциала, необходимого для самостоятельного контроля, анализа и рекомендаций по выработке мер, привлекаются сторонние организации, обладающие необходимым опытом, знаниями и компетенцией.

РАЗДЕЛ 7.1. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТАХ, НЕ ИМЕЮЩИХ ПОДКЛЮЧЕНИЯ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных на автоматизированном рабочем месте, не имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих угроз:

- угроз утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угроз несанкционируемым допуском данных, обрабатываемым в автоматизированном рабочем месте.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСД, возможно при наличием функций голосового ввода данных в ИСД или функций воспроизведения данных акустическими средствами ИСД.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСД.

Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

МОДЕЛЬ Угрозы НСД в автономном АРМ связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД. Кроме этого, источниками угроз НСД к информации в АРМ могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСД на базе автономного АРМ возможны все виды уязвимостей ИСД, за исключением уязвимостей, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных. В таких ИСД возможны:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ.

РАЗДЕЛ 7.2. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТАХ, ИМЕЮЩИХ ПОДКЛЮЧЕНИЕ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБД:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угрозы несанкционированного доступа к данным, обрабатываемым на автоматизированном рабочем месте.

Возникновение УБД в рассматриваемых ИСД по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в ИСД связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД, а также нарушителей, не имеющих доступа к ИСД, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСД, связанные с действиями нарушителей, имеющих доступ к ИСД, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

РАЗДЕЛ 7.3. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ЛОКАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ДАННЫХ, НЕ ИМЕЮЩИХ ПОДКЛЮЧЕНИЯ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных в локальных ИСД, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБД:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угрозы НСД к данных, обрабатываемым на автоматизированном рабочем месте.

Возникновение УБД в рассматриваемых ИСД по техническим каналам характеризуется теми же условиями и факторами, что и для локальных ИСД, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в локальных ИСД связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД.

Угрозы НСД в ИСД, связанные с действиями нарушителей, имеющих доступ к ИСД, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Кроме того, в такой ИСД могут иметь место:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;
- угрозы выявления паролей;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

РАЗДЕЛ 7.4. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ ОБРАБАТЫВАЕМЫХ В ЛОКАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ДАННЫХ, ИМЕЮЩИХ ПОДКЛЮЧЕНИЕ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных в локальных ИСД, имеющих подключение к сетям связи общего

пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБД:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угрозы НСД к данным, обрабатываемым на автоматизированном рабочем месте.

Возникновение УБД в рассматриваемых ИСД по техническим каналам характеризуется теми же условиями и факторами, что и для предыдущих типов ИСД.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД, а также нарушителей, не имеющих доступа к ИСД, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСД, включают в себя угрозы, аналогичные тем, которые реализуются в отдельном АРМ, не имеющем подключения к сетям связи общего пользования.

Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы ИСД, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

РАЗДЕЛ 7.5. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ДАННЫХ, НЕ ИМЕЮЩИХ ПОДКЛЮЧЕНИЯ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных в распределенных ИСД, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБД:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угрозы НСД к данным, обрабатываемым на автоматизированном рабочем месте.

Возникновение УБД в рассматриваемых ИСД по техническим каналам характеризуется теми же условиями и факторами, что и для предыдущих типов ИСД.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД.

При этом могут быть угрозы, аналогичные тем, которые имеют место в отдельном АРМ, не подключенном к сетям общего пользования, а также угрозы, реализуемые внутри распределенной сети с использованием протоколов межсетевого взаимодействия, в том числе:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;
- угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;
- угрозы внедрения ложного объекта сети;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

РАЗДЕЛ 7.6. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ДАННЫХ, ИМЕЮЩИХ ПОДКЛЮЧЕНИЕ К СЕТЯМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА.

При обработке данных в распределенных ИСД, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБД:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.
- угрозы НСД к данным, обрабатываемым на автоматизированном рабочем месте.

Возникновение УБД в рассматриваемых ИСД по техническим каналам характеризуется теми же условиями и факторами, что и для предыдущих типов ИСД.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСД, включая пользователей ИСД, реализующих угрозы непосредственно в ИСД, а также нарушителей, не имеющих доступа к ИСД, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСД, аналогичны тем, которые имеют место в распределенных ИСД, не имеющей подключения к сетям общего пользования. Кроме того, в такой ИСД имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСД и принимаемой в ИСД из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСД, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы внедрения ложного объекта как в ИСД, так и во внешних сетях;
- угрозы подмены доверенного объекта;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

ГЛАВА 8. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА И ЕГО ВОССТАНОВЛЕНИЯ ПОСЛЕ ПРЕРЫВАНИЙ

8.1. В случае возникновения в информационной инфраструктуре Организации зафиксированных нештатных ситуаций (аварий или существенного снижения функциональности компонентов информационной инфраструктуры), при которых временно отсутствует техническая возможность применения всех мер защиты информации, входящих в систему защиты информации, Организация, в лице ответственных работников, осуществляет действия, направленные на выполнение своих служебных обязанностей в условиях отсутствия применения отдельных мер защиты информации, а также должный контроль указанных действий.

8.2. Информационные активы, существенные для обеспечения непрерывности бизнеса

Критичная (жизненно–важная) информация Организации

С позиции обеспечения целостности и доступности, вся информация в Организации по уровням важности разделяется на следующие категории:

а) критичная жизненно–важная информация, защищённость которой является необходимым условием функционирования Организации;

б) чувствительная важная информация, потеря или модификация которой приводит к материальному ущербу для Организации.

Защите подлежат информационные ресурсы, выбранные в качестве объектов защиты.

С точки зрения информационной безопасности, приоритетными направлениями и объектами защиты в Организации являются:

1) обеспечение целостности и доступности критичной (жизненно–важной) и чувствительной информации;

2) защита от несанкционированного доступа к конфиденциальной информации и информации для служебного пользования.

Для обеспечения непрерывности бизнеса существенными являются такие информационные активы, как:

- платежный технологический процесс;
- платежная информация.

8.3. Требования по обеспечению ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания

С целью обеспечения непрерывности бизнеса в Организации для АС, обрабатывающих критичную информацию, обеспечивается сохранение (восстановление) их работоспособности в том числе при утере, уничтожении, несанкционированной модификации данных, программного обеспечения, выходе из строя оборудования и т.п.

1) Для поддержания работоспособности АИС проводится постоянная работа по следующим направлениям:

- сопровождение работы пользователей;
- сопровождение работы аппаратного и программного обеспечения;
- резервное копирование;
- документирование;
- регламентные (профилактические) работы.

2) 3) Сопровождение работы аппаратного и программного обеспечения предусматривает:

- контроль за несанкционированной установкой аппаратного или программного обеспечения;
- контроль за несанкционированным изменением программ и прав доступа к ним;
- хранение эталонных копий программ, в том числе и предыдущих версий, в специальных библиотеках программного обеспечения;
- разделение технологических процессов разработки и эксплуатации программного обеспечения;
- контроль и документирование любых изменений аппаратной и программной частей АС, отражение изменений в прикладном программное обеспечении в номере версии.

4) Резервное копирование информации должно удовлетворять следующим требованиям:

- обеспечивать возможность восстановления программ и данных в случае возникновения аварийной ситуации;
- копии программного обеспечения и данных должны располагаться в безопасном месте;
- периодически должна проверяться возможность восстановления информации с копий;
- копирование информации должно проводиться в соответствии с разработанным для этого регламентом.

5) Процедуры резервного копирования данных осуществляются в строгом соответствии с регламентом. Периодичность резервного копирования должна позволять восстановить работу АС без существенных потерь для Организации.

6) АС, обрабатывающие критичную информацию, должны иметь резервные центры обработки, способные поддерживать работу информационных систем в случае выхода из строя основных центров.

7) Резервированию подлежит:

- серверное и сетевое оборудование;
- программное обеспечение;
- информационные базы данных.

8) Серверное оборудование, осуществляющее хранение и обработку критичной информации, должно располагаться в физически безопасном помещении, оборудованном средствами защиты от несанкционированного доступа, средствами сигнализации и пожаротушения.

8.4. Обеспечение непрерывности бизнеса и его восстановления после возможного прерывания в Организации должно осуществляться согласно Плану:

1) в случае возникновения кризисной ситуации, несущей угрозу непрерывности критичного процесса, обнаружившее её лицо обязано уведомить об этом СА и руководство Организации;

2) СА с привлечением других работников, задействованных в возникновении кризисной ситуации, должны осуществить действия по её локализации и выявления нарушения, приведшего к критической ситуации;

3) немедленная реакция на нарушение действие пользователей и персонала в момент обнаружения нарушения;

4) возобновление обработки после устранения нарушения и первичного восстановления, либо после переключения на резервную систему;

5) полная проверка системы на предмет отсутствия причин, ведущих к возникновению кризисной ситуации;

6) полное восстановление функционирования системы с осуществлением следующих процедур: удаление и замена поврежденных компонентов системы, проверка целостности и доступности программных и аппаратных средств, данных, возобновление обработки в полном объеме;

7) оценка ущерба от нарушения, расследование причин возникновения кризисной ситуации.

Для проверки реагирования работников в критических ситуациях План должен периодически (не реже 1 раза в год) тестироваться. Тестирование и проверка отработки Плана в реальных условиях производится администратором ИБ.

Работники должны также проходить ежегодное обучение навыкам реагирования на угрозы непрерывности бизнеса и его восстановления после возможного прерывания.

Ответственным за реализацию Плана, а также за проведение обучения и повышение осведомленности работников возложено на СА.

8.5. Выполнение Плана, в том числе восстановление после прерывания, основывается на документально оформленных результатах оценки рисков нарушения ИБ применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

8.6. В Организации реализованы защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания:

- определение информации, содержащей коммерческую тайну, и сроков ее действия;
- категорирование помещений по степени важности обрабатываемой в них информации;
- определение категории информации, обрабатываемой каждой отдельной системой;
- описание системы, определение факторов риска, определение уязвимых мест систем;
- выбор средств и мер защиты для предотвращения воздействия факторов риска и их минимизации;
- выбор средств и мер контроля и управления для своевременной локализации и минимизации воздействия факторов риска.

Реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания должны основываться на соответствующих требованиях по обеспечению ИБ.

8.7. План обеспечения непрерывности бизнеса и его восстановления после прерывания должен быть согласован с существующими в Организации процедурами обработки инцидентов ИБ.

8.8. Периодическое тестирование Плана обеспечения непрерывности бизнеса и его восстановления после прерывания выполняется с привлечением всех подразделений по решению СА или иного уполномоченного лица. По результатам тестирования при необходимости проводится соответствующая корректировка Плана. Сценарий тестирования должен быть составлен с учетом существующей в Организации модели угроз и нарушителей, а также результатов оценки рисков.

8.9. Администратором ИБ или иным уполномоченным лицом должна быть реализована программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний.

8.10. План обеспечения непрерывности бизнеса и его восстановления после прерывания для обеспечения уверенности в их эффективности подлежит регулярному пересмотру и обновлению. Процедуры пересмотра и обновления Плана должны производится с учетом изменений в приоритетах, целях и интересах бизнеса Организации; пересмотра моделей угроз; оценки рисков нарушения ИБ.

8.11. Разработка плана обеспечения непрерывности бизнеса и его восстановления после прерывания в возлагается на СА. Ответственные за выполнение указанной обязанности возлагается на СА.

ГЛАВА 9. ПОРЯДОК КОНТРОЛЯ И СОВЕРШЕНСТВОВАНИЯ МЕР ЗАЩИТЫ

ИНФОРМАЦИИ ОРГАНИЗАЦИИ

РАЗДЕЛ 9.1. ПРОЦЕДУРЫ КОНТРОЛЯ РАБОТОСПОСОБНОСТИ (ФУНКЦИОНИРОВАНИЯ, ЭФФЕКТИВНОСТИ) РЕАЛИЗОВАННЫХ В АС ЗАЩИТНЫХ МЕР

На стадии эксплуатации АС должны выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в АС защитных мер:

Процедуры контроля нарушения работоспособности (функционирования, эффективности) реализованных в АС защитных мер	Факторы, позволяющие выявить недостатки
Проверка отсутствия сбоя и отказов технических средств и каналов связи	Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Проверка отсутствия нарушения функциональности криптографической системы	Случайное или намеренное неправильное управление ключами, криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности информации, нарушению неотказуемости приема передачи информации, блокировке функционирования платежных и информационных систем
проверка отсутствия нарушения функциональности архивной системы	Нарушение конфиденциальности и целостности архивных данных и/или непредоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы

РАЗДЕЛ 9.2. ТРЕБОВАНИЯ К ВЫБОРУ/КОРРЕКЦИИ ПОДХОДА К ОЦЕНКЕ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОВЕДЕНИЮ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.2.1. Методика оценки рисков нарушения ИБ определяет способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания:

- степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя в результате их воздействия на объекты среды информационных активов (типов информационных активов);
- степени тяжести последствий от потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов (типов информационных активов).

Порядок оценки рисков нарушения ИБ определяет необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения:

1) В основе исходной концептуальной схемы ИБ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными активами. Если злоумышленнику удается установить такой контроль, то как самому Организации, так и клиентам, которые доверили ей свои собственные активы, наносится ущерб.

Под злоумышленником здесь понимается лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

2) Наибольшими возможностями для нанесения ущерба Организации обладает его

собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником. Поэтому этими отношениями необходимо управлять. Понимая, что наиболее критичным элементом безопасности организации является его персонал, собственник должен всемерно поощрять заинтересованность и осведомленность персонала в решении проблем ИБ.

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает.

3) Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри Организации.

Практически никогда не известно о готовящемся нападении, оно, как правило, бывает неожиданным. Нападения, как правило, носят локальный и конкретный по месту, цели и времени характер.

Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем выявления уязвимостей ИБ. Путем поиска или создания уязвимостей ИБ он отрабатывает наиболее эффективный метод нападения (получения контроля над активом).

9.2.2. В Организации определены такие основные критерии принятия рисков нарушения ИБ как:

- степень защищенности информационных ресурсов от негативного влияния внешних и внутренних факторов;
- квалификация и подготовка работников;
- степень соответствия используемых технических и технологических решений характеру и масштабам деятельности.

Уровень допустимого целевого остаточного риска нарушения ИБ рассматривается Организацией в качестве одного из основных параметров, оказывающих непосредственное влияние на возникновение (увеличение) таких рисков как операционный риск, кредитный риск, правовой риск и риск потери деловой репутации, а также косвенно влияющий на возникновение (увеличение) иных рисков. Он не должен выходить за рамки информационно безопасной работы для самого Организации, его работников и третьих лиц.

9.2.3. Методика оценки рисков нарушения ИБ основывается на том, что оценка уровня информационной безопасности, своевременное выявление факторов, влияющих на снижение показателей информационной безопасности, разработка мер по поддержанию должного уровня безопасности в соответствии с характером и масштабами деятельности в настоящем, а также с учетом перспектив развития рассматриваются Организацией в качестве существенных направлений осуществления внутреннего контроля.

9.2.4. Оценка рисков нарушения ИБ проводится для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ.

9.2.5. В Организации создается и поддерживается в актуальном состоянии единый информационный ресурс (база данных), содержащая информацию об инцидентах ИБ.

9.2.6. Полученные в результате оценивания рисков нарушения ИБ величины рисков должны быть соотнесены с уровнем допустимого риска, принятого в Организации.

9.2.7. Обязанность по определению/коррекции методики оценки рисков нарушения ИБ/подхода к оценке рисков нарушения ИБ в Организации, возложена на СА. Ответственным за выполнение указанных действий является СА.

Квалификация и подготовка работников в части оценки влияния на уровень информационной безопасности, их роли в СОИ, рассматриваются с точки зрения соответствия характеру возлагаемых на работников должностных обязанностей; знания принципов профессиональной этики, ознакомления с параметрами конфиденциальности информации и отнесения сведений к тайне об операциях клиентов, а также ответственности за нарушение указанных принципов и параметров, злоупотреблений и противоправных действий, связанных с несанкционированным использованием информации.

9.2.8. Обязанность по оценке рисков нарушения ИБ в Организации, возложена на СА. Ответственным за выполнение указанных действий является СА.

РАЗДЕЛ 9.3. ТРЕБОВАНИЯ К РАЗРАБОТКЕ ПЛАНОВ ОБРАБОТКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.3.1. По каждому из рисков нарушения ИБ, который является недопустимым, Организация вправе определить план, определяющий один из возможных способов его обработки:

- перенос риска на сторонние организации (например, путем страхования указанного риска);
- уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);
- осознанное принятие риска;
- формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирования планов по их реализации.

9.3.2. Планы обработки рисков нарушения ИБ должны быть согласованы с СА, и утверждены руководством.

9.3.3. Планы реализаций требований по обеспечению ИБ должны содержать последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер.

9.3.4. Обязанность по разработке планов обработки рисков нарушения ИБ в Организации возложена на СА. Ответственным за выполнение указанных действий является СА.

РАЗДЕЛ 9.4. ТРЕБОВАНИЯ К РАЗРАБОТКЕ/КОРРЕКЦИИ ВНУТРЕННИХ ДОКУМЕНТОВ, РЕГЛАМЕНТИРУЮЩИХ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.4.1. Разработку/коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ в Организации, Организация проводит с учетом рекомендаций по стандартизации Банка России.

9.4.2. В Организации должны разрабатываться/корректироваться следующие внутренние документы:

политика ИБ;

частные политики ИБ (при наличии необходимости);

документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ (при наличии необходимости).

9.4.3. В рабочем режиме в Организации должны определяться/корректироваться:

- цели и задачи обеспечения ИБ: целью и задачей деятельности в рамках процессов управления информационной безопасностью является обеспечение безопасности работы всех подразделений, связанной с угрозами в информационной сфере;
- основные области обеспечения ИБ;
- назначение и распределение ролей и доверия к персоналу;
- обеспечения информационной безопасности при работе с АС;
- защиты от НСД и НРД, управления доступом и регистрацией всех действий при работе с АС и ЭВМ;
- антивирусная защита;
- использование ресурсов сети Интернет;
- использование средств криптографической защиты информации;
- защита платежных и информационных технологических процессов.
- типы основных защищаемых информационных активов:

1) работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;

2) различные виды информации платежная, финансово-аналитическая, служебная, управляющая и пр.;

3) Бизнес процессы (платежные технологические процессы, информационные технологические процессы);

4) продукты и услуги, предоставляемые клиентам.

- модели угроз и нарушителей: на каждом из уровней информационной инфраструктуры угрозы и их источники, а также методы и средства защиты являются различными.

1) Главной целью злоумышленника является получение контроля над информационными

активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например, путем раскрытия конфиденциальной аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению «затраты/получаемый результат».

2) Другими целями злоумышленника могут являться, например, нарушение функционирования бизнес-процессов путем нарушения доступности или целостности информационных активов, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

3) Основными источниками угроз ИБ являются:

– неблагоприятные события природного, техногенного и социального характера;
– террористы и криминальные элементы;
– зависимость от поставщиков/провайдеров/партнеров/клиентов;
– сбои, отказы, разрушения/повреждения программных и технических средств;
– работники, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
– работники, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
– несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

4) Наиболее актуальными источниками угроз на физическом, сетевом уровнях и уровне сетевых приложений являются:

– внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие атаки; лица, осуществляющие попытки НСД и НРД;
– внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
– сбои, отказы, разрушения/повреждения программных и технических средств.

5) Самыми актуальными источниками угроз на уровнях операционных систем, систем управления базами данных, технологических процессов являются:

− внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи приложений и технологий, администраторы ИБ и т.д.;
− комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре.

6) Наиболее актуальные источники угроз на уровне бизнес-процессов:

– внутренние нарушители ИБ: авторизованные пользователи и работники - пользователи АС, представители менеджмента организации и пр.;
– комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
– несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

7) Любой из видов угроз информационной безопасности непосредственно влияет на операционные, правовые риски деятельности, которые в свою очередь сказываются на бизнес-процессах организации;

− совокупность правил, требований и руководящих принципов в области ИБ: требования, правила и руководящие принципы в области ИБ регламентированы и содержатся в законодательных актах, нормативных правовых актах Банка России, локальных правовых актах, в том числе настоящей Политики, и подлежат корректировке на регулярной основе с учетом анализа фактических обстоятельств;
− основные требования по обеспечению ИБ: стратегия обеспечения ИБ заключается как в эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников, так и в регулярном пересмотре политики ИБ, а также корректировке СОИБ. В случае реализации угроз должен быть использован разработанный план действий, позволяющий свести к минимуму возможные потери и восстановить СОИБ.

- принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;

Для реализации и поддержания ИБ реализуются четыре группы процессов:

- планирование СОИБ («планирование»);
- реализация СОИБ («реализация»);
- мониторинг и анализ СОИБ («проверка»);
- поддержка и улучшение СОИБ («совершенствование»).
- Указанные группы процессов составляют СМИБ.
- основные принципы повышения уровня осознания и осведомленности в области ИБ:

Степень выполнения указанной деятельности со стороны руководства Организации определяется осознанием необходимости обеспечения ИБ. Осознание необходимости обеспечения ИБ проявляется в использовании руководством Организации бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса организации с допустимыми рисками;

- принципы реализации и контроля выполнения требований политики ИБ: руководству необходимо инициировать, поддерживать и контролировать выполнение процессов СОИБ.

9.4.4. Разработка/корректировка внутренних документов, регламентирующих деятельность в области обеспечения ИБ, проводится на основе:

- законодательства Российской Федерации;
- нормативных актов и предписаний регулирующих и надзорных органов;
- договорных требований со сторонними организациями;
- результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов).

9.4.5. Совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна содержать требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ.

9.4.6. Свидетельством выполнения Организацией деятельности в области обеспечения ИБ является то, что применяемые Организацией технологии осуществления операций и сделок, алгоритмы их автоматизации и защиты, средства информационной защиты, техническая база, в том числе оборудование помещений, минимизация возможность нарушения работоспособности, непрерывности работы и восстановления функционирования всех систем, в том числе и в случае технических или технологических сбоев, при попытках внешнего проникновения.

Ответственность работников за выполнение этой деятельности определяется в зависимости от занимаемой должности и класса информационного актива, с которым связано выполнение служебных обязанностей подразделения, в котором трудится работник. Ответственность возникает в случае невыполнения требований законодательства, нормативных правовых актов Банка России, локальных правовых актов в области обеспечения ИБ. Степень и размер ответственности определяются в соответствии с Федеральными законами, регламентирующими взыскания с работников в случае нарушения ими действующего законодательства и обязательств перед Организацией.

9.4.7. Для эффективного выполнения целей и задач в области обеспечения ИБ, выделены и определены соответствующие функции (роли) персонала. Функции персонифицированы с установлением ответственности за их исполнение, которая обозначена в должностных инструкциях работников. Формирование ролей осуществляется на основании бизнес-процессов, и начинается со стадии приема на работу в Организацию. При этом выполняются следующие процедуры проверки:

- идентификация личности,
- соответствие заявляемой квалификации,
- точность и полнота биографических данных,
- наличие рекомендаций.

Лиц, которых предполагается принять на работу, начальник подразделения в ходе устной беседы подвергает проверке в части профессиональных навыков и оценки профессиональной пригодности.

Далее распределение ролей осуществляется в зависимости от стоящих перед Организацией текущих и долгосрочных задач.

РАЗДЕЛ 9.5. ТРЕБОВАНИЯ К ПРИНЯТИЮ РУКОВОДСТВОМ ОРГАНИЗАЦИИ РЕШЕНИЙ О РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.5.1. Решения о реализации и эксплуатации СОИБ должны утверждаться руководством. В частности, в Организации, при наличии необходимости, документально оформляются решения руководства:

- об анализе и принятии остаточных рисков нарушения ИБ;
- о планировании этапов внедрения СОИБ, в частности, требований по обеспечению ИБ, изложенных в стандартах Банка России;
- о распределении ролей в области обеспечения ИБ;
- о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований Стандартов Банка России и снижение рисков ИБ;
- о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

9.5.2. Все планы внедрения СОИБ должны быть утверждены руководством. Указанные планы должны документально фиксировать:

- последовательность выполнения мероприятий в рамках указанных планов;
- сроки начала и окончания запланированных мероприятий;
- должностных лиц (подразделения), ответственных за выполнение каждого указанного мероприятия.

9.5.3. Планы по обеспечению ИБ :

- разрабатываются в случае выявления необходимости приведения действий подразделений, информационных и иных материальных активов, в соответствие с требованиями законодательства и нормативных правовых актов Банка России, а также локальных правовых актов службой информационной безопасности в Организации. Служба информационной безопасности осуществляет также контроль за их исполнением;
- при наличии соответствующих указаний и рекомендаций Банка России, а также в силу технической и служебной необходимости службой информационной безопасности осуществляется их пересмотр, либо введение в действие новых планов.

9.5.4. В Организации должны быть документально оформлены решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ.

РАЗДЕЛ 9.6. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ РЕАЛИЗАЦИИ ПЛАНОВ ВНЕДРЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.6.1. В соответствии с вводимыми планами реализаций требований по обеспечению ИБ, в Организации, при появлении угроз в отношении ИБ должны быть документально определены и выполняться проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами.

9.6.2. Для построения элементов СИБ применительно к конкретной области или сфере деятельности должны быть реализованы конкретные защитные меры, применяемые к объектам среды в соответствии с существующими в Организации требованиями по обеспечению ИБ, сформулированными в политике ИБ и других внутренних документах.

9.6.3. Распорядительным актом по Организации должны быть документально определены роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер, и назначены ответственные за выполнение указанных ролей.

РАЗДЕЛ 9.7. ТРЕБОВАНИЯ К РАЗРАБОТКЕ И ОРГАНИЗАЦИИ РЕАЛИЗАЦИИ ПРОГРАММ ПО ОБУЧЕНИЮ И ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.7.1. Администратором ИБ (при его наличии, или СА, или иным уполномоченным лицом) должна быть организована утвержденная руководством работа с персоналом в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

9.7.2. В планах обучения и повышения осведомленности должны быть установлены требования

к периодичности обучения и повышения осведомленности.

9.7.3. Программы обучения и повышения осведомленности должны включать информацию:

- по существующим политикам ИБ;
- по применяемым в Организации защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами;
- о значимости и важности деятельности работников для обеспечения ИБ.

9.7.4. Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области ИБ, соответствующее полученной роли.

9.7.5. Разработкой, реализацией планов и программ обучения и повышения осведомленности в области ИБ и контролем результатов в Организации занимается СА. Ответственным за выполнение указанных действий является СА или иное уполномоченное лицо.

РАЗДЕЛ 9.8. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.8.1. Процедуры обработки инцидентов в Организации включают в себя следующие:

- процедуры обнаружения инцидентов ИБ:

идентификация инцидента наиболее важная и сложная часть процедуры обработки инцидента. Очевидные события (несанкционированное изменение содержимого) события означавшие либо вторжение, либо просто ошибку пользователя (например, удаление файлов). С целью обнаружения инцидентов в Организации должны быть реализованы следующие мероприятия:

- на всех серверах должны быть включены функции протоколирования.
- Должны быть включены средства информирования СА на межсетевых экранах и других средствах управления доступом.
- В местах концентрации сетевого трафика должны быть установлены средства обнаружения атак, следящие за появлением в трафике признаков атак.
- Должны выполняться периодические проверки целостности межсетевых экранов и других систем управления доступом.
- Системы обнаружения атак должны периодически проверяться на предмет правильной конфигурации, корректности работы, актуальности ПО и баз знаний известных сетевых уязвимостей.

- процедуры информирования об инцидентах;

При любом выявлении инцидента (обнаруженном вирусе, изменении конфигурации, необычном поведении компьютера или программы):

- пользователи обязаны информировать СА;
- СА информирует руководство о наличии инцидента;
- СА предупреждает всех пользователей, имеющих доступ к программам и данным, к которым имеет отношение инцидент, о его наличии, и о работе их компьютеров в аварийном режиме;
- любой компьютер, который подозревается в заражении вирусом, немедленно отключается от сети;
- зараженный компьютер не подключается к сети до тех пор, пока системные администраторы не удостоверятся в успешном результате лечения;
- если опасность устранить не удается, все программы в компьютере удаляются, включая, при необходимости, загрузочные модули операционной системы;
- удаленные программы повторно устанавливаются из надежных источников и повторно проверяются;
- проводится анализ причин возникновения инцидента, и принимаются необходимые меры безопасности.

- процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ:

СА производит служебное расследование, по результатам которого руководителю направляется отчет, включающий в себя:

- описание произошедшего инцидента;
- оценка ущерба от нарушения (утраченные программы и файлы, повреждение аппаратуры, потери времени на восстановление атакованных систем и т.п.);
- оценка действий персонала и эффективность средств защиты информации;
- виновные в нарушении информационной безопасности.

- процедуры реагирования на инцидент:

СА принимает ответные меры, которые включают в себя:

– сдерживание ограничение атакуемой области, принятие решения о дальнейшей работе системы;

– ликвидацию нарушения;

– восстановление нормальной работы системы;

– при необходимости, по факту нарушения информационной безопасности проводится служебное расследование.

Решение о наказании виновных в нарушении информационной безопасности или передаче материалов по данному инциденту в правоохранительные органы принимает Руководитель Организации.

− процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ): после ликвидации нарушения режима информационной безопасности службой ИБ принимаются меры направленные на предотвращение подобных инцидентов в дальнейшем:

– производится анализ причин инцидентов и достаточность принятых мер по защите информации;

– пересматривается, если признано необходимым, действующая политика безопасности;

– устанавливаются, если признано необходимым, дополнительные средства защиты информации.

9.8.2. В СА должна быть сформирована и поддерживаться в актуальном состоянии централизованная база данных инцидентов ИБ. Информация об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ должна храниться в Организации.

Информация должна быть обобщена в электронном журнале с указанием:

– даты возникновения инцидента;

– его причины;

– процедуры реагирования на инцидент.

9.8.3. Действия работников при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях производятся в порядке, установленном настоящей Политики. Работники должны быть осведомлены об указанных порядках.

9.8.4. Процедуры расследования инцидентов ИБ должны учитывать действующее законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов в области ИБ.

9.8.5. В Организации должны приниматься и выполняться документально оформленные решения по всем выявленным инцидентам ИБ.

9.8.6. Ответственными за обнаружение, классификацию, реагирование, анализ и расследование инцидентов ИБ является СА. Ответственным за выполнение указанных действий является СА или иное уполномоченное лицо.

РАЗДЕЛ 9.9. ТРЕБОВАНИЯ К УЛУЧШЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

9.9.1. Процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты в Организации могут включать следующие мероприятия:

− на всех серверах должны быть включены функции протоколирования.

− Должны быть включены средства информирования СА на межсетевых экранах и других средствах управления доступом.

− В местах концентрации сетевого трафика должны быть установлены средства обнаружения атак, следящие за появлением в трафике признаков атак.

− Должны выполняться периодические проверки целостности межсетевых экранов и других систем управления доступом.

− Должен проводиться ежедневный анализ журналов протоколирования систем управления доступом.

− Должен проводиться ежедневный анализ системных журналов серверов внутренней сети.

− Системы обнаружения атак должны периодически проверяться на предмет правильной конфигурации, корректности работы, актуальности ПО и баз знаний известных сетевых уязвимостей.

− Должна быть установлена автоматизированная система антивирусной безопасности с актуальными базами данных, осуществляющая антивирусный контроль передаваемой по сети и хранимой на серверах информации.

Указанные процедуры должны проводиться администратором ИБ и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ.

9.9.2. Результаты выполнения процедур мониторинга СОИБ и контроля защитных мер должны документально фиксироваться.

9.9.3. В Организации должны выполняться процедуры сбора и хранения информации о действиях работников, событиях и параметрах, имеющих отношение к функционированию защитных мер.

Архивирование информации должно обеспечивать сохранение юридически значимой и другой представляющей ценность для информации, возможность разрешения спорных ситуаций и проведения расследований в случаях нарушений информационной безопасности.

Архивированию подлежат:

− электронные документы;

− электронные образы бумажных документов;

− электронные протоколы (журналы информационной безопасности, регистрационные журналы, log–файлы и т.п.) работы АС;

− ключи, открытые ключи ЭЦП подписи и шифрования;

− любая другая информация в электронном виде, для которой определена необходимость архивирования.

Для каждого архива должен быть определен порядок его ведения, в котором устанавливаются технология, периодичность обновления и срок хранения информации.

Электронные архивы должны удовлетворять следующим требованиям:

− архив не доступен для записи или удаления информации любым лицом, кроме ответственного за ведение архива;

− документы в архиве хранятся со всеми возможными подтверждениями их подлинности, в частности, с ЭЦП (для документов, которые были подписаны ЭЦП);

− архив надежно защищен от утраты и уничтожения (дублирование, хранение в несгораемых сейфах и кладовых, выбор носителей соответствующей надежности);

− конфиденциальная информация хранится в архиве в зашифрованном виде.

9.9.4. Информация обо всех инцидентах, выявленных в процессе мониторинга СОИБ и контроля защитных мер, должна включаться в базу данных инцидентов ИБ.

9.9.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть следующим:

− Сетевой мониторинг и системный аудит предназначен для просмотра информации о работающих пользователях, записи информации о возникающих ошибках на различных рабочих станциях. На основе анализа текущего мониторинга администратор ИБ делает вывод о необходимости пересмотра процедур мониторинга.

− Данные, полученные в результате сетевого мониторинга используются для выявления «слабых» рабочих мест в сети, а на их основе о необходимости внесения изменения в список процедур мониторинга.

− Наличие системного аудита позволяет выявить возможные нарушения режима информационной безопасности, определять причины нарушения, а также находить (и потом устранять) потенциально слабые места в системе безопасности. Кроме того, наличие аудита в системе играет роль сдерживающего фактора: многие, зная, что их действия фиксируются, не будут совершать наказуемых действий. В этой связи необходимо учащать процедуры, либо проводить их реже.

− Сетевой мониторинг и системный аудит предоставляется с помощью специализированного программного обеспечения. Соответственно необходимо вносить изменения в список программного обеспечения, с помощью которого осуществляется мониторинг.

9.9.6. Процедуры мониторинга СОИБ и контроля защитных мер в Организации, а также пересмотром указанных процедур, выполняются СА.

Ответственность за мониторинг СОИБ и контроля защитных мер в Организации, а также за пересмотр указанных процедур возлагается на администратора информационной безопасности.

РАЗДЕЛ 9.10. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ САМООЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.10.1. Самооценка ИБ проводится в соответствии со стандартами Банка России.

9.10.2. Программа самооценок ИБ состоит из:

- планирования самооценок ИБ;
- организации,
- их контроля,
- анализа;
- совершенствования,
- обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ

в заданные сроки.

С целью реализации такой программы администратор ИБ не реже одного раза в год, при наличии угроз ИБ или нарушений и сбоев в работе АС производит действия программы по осуществлению самооценки ИБ, подготавливает отчет для руководства.

9.10.3. С целью реализации программы, указанной в пункте 6.3.2 настоящей Политики СА не реже одного раза в год производит действия программы по осуществлению самооценки ИБ

9.10.4. Для каждой проводимой в Организации самооценки ИБ необходим план проведения самооценки, определяющий:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- порядок и сроки выполнения мероприятий самооценки ИБ;
- распределение ролей среди работников БС, связанных с проведением самооценки ИБ.

9.10.5. По результатам проведения самооценок ИБ СА подготавливает отчет и передает его для ознакомления руководству.

9.10.6. Программу самооценок ИБ выполняет СА.

Ответственность за проведение самооценок в Организации, а также за наличие отчетов о выполнении самооценок несет СА или иное уполномоченное лицо.

РАЗДЕЛ 9.11. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.11.1. Аудит ИБ должен проводиться в случаях, установленных законом, нормативными правовыми актами Банка России, а также при наличии необходимости проверки действующей в организации системы ИБ.

9.11.2. Организацию аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки, осуществляет СА в соответствии с договором с аудиторской организацией.

9.11.3. Для каждого проводимого аудита ИБ необходимо оформить план аудита, определяющий:

- цель аудита ИБ;
- критерии аудита ИБ;
- область аудита ИБ;
- дату и продолжительность проведения аудита ИБ;
- состав аудиторской группы;
- описание деятельности и мероприятий по проведению аудита;
- распределение ресурсов при проведении аудита.

9.11.4. С целью проведения аудита в Организации должны быть оформлены договоры с аудиторскими организациями.

9.11.5. Полученные в результате проведения аудита ИБ материалы хранятся вместе с отчетом о проведении аудита. доступ к указанным материалам получают лица, заинтересованные в их использовании в соответствии с порядком работы с документами, содержащими сведения ограниченного распространения»;

9.11.6. Переговоры с аудиторской организацией в процессе проведения аудита ИБ, действия по предоставлению представителям аудиторской организации необходимых материалов и техники, получение результатов аудиторской проверки ИБ проводит СА по согласованию с руководством;

9.11.7. При необходимости непосредственно обратиться к руководству СА по требованию

представителей аудиторской организации согласуют дату и время их встречи с руководством;

9.11.8. Опрос работников может производиться аудиторской организацией только после согласования с руководством после проведения СА и юридической службы необходимого инструктажа и при их непосредственном участии.

9.11.9. Наблюдения за деятельностью работников со стороны представителей аудиторской организации может производиться аудиторской организацией только в случаях, установленных законом, после согласования с руководством после проведения СА и юридической службы необходимого инструктажа и при их непосредственном участии.

9.11.10. По результатам проведения аудита должны быть подготовлены отчеты. Результаты аудитов, а также соответствующие отчеты должны быть доведены до руководства.

9.11.11. Полученные в результате проведения аудита ИБ материалы хранятся вместе с отчетом о проведении аудита. Доступ к указанным материалам получают лица, заинтересованные в их использовании в соответствии с порядком работы с документами, содержащими сведения ограниченного распространения».

9.11.12. Организацию выполнения программ аудитов и планов отдельных аудитов проводит СА по согласованию с руководством; ответственным за выполнение указанных действий является СА.

РАЗДЕЛ 9.12. ТРЕБОВАНИЯ К АНАЛИЗУ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.12.1. В Организации должен проводиться анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах;
- данные об изменениях вне, например, данные об изменениях в законодательстве Российской Федерации, изменениях в договорных обязательствах.

9.12.2. Анализ функционирования СОИБ должен включать в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в Организации, требованиям законодательства Российской Федерации, нормативным правовым актам Банка России, контрактным требованиям;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в Организации, требованиям политик ИБ;
- оценку адекватности модели угроз существующим угрозам ИБ;
- оценку рисков в области ИБ, включая оценку уровня остаточного и допустимого риска;
- проверку адекватности используемых защитных мер требованиям внутренних документов Организации и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

9.12.3. Результаты анализа функционирования СОИБ должны анализироваться.

9.12.4. Действия, связанные с процедурами анализа функционирования СОИБ, осуществляются СА, ответственным за выполнение указанных действий является СА.

РАЗДЕЛ 9.13. ТРЕБОВАНИЯ К АНАЛИЗУ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ РУКОВОДСТВА

9.13.1. Для формирования информации с целью проведения анализа СОИБ в Организации руководству должны быть определены:

- результаты мониторинга СОИБ и контроля защитных мер;
- результаты анализа функционирования СОИБ;
- результаты аудитов ИБ;
- результаты самооценок ИБ;
- информация о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;

− информация о новых выявленных уязвимостях и угрозах ИБ;
− информация о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
− информация об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России;
− информация по выявленным инцидентам ИБ;
− анализ выполнения требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков;
− выполнение требований непрерывности бизнеса и его восстановления после прерывания.

9.13.2. В организации должны быть определены роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством, и назначены ответственные за выполнение указанных ролей.

РАЗДЕЛ 9.14. ТРЕБОВАНИЯ К ПРИНЯТИЮ РЕШЕНИЙ ПО ТАКТИЧЕСКИМ УЛУЧШЕНИЯМ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ОБЕСПЕЧЕНИЕ РЕСУРСАМИ)

9.14.1. Для принятия решений, связанных с тактическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:
− аудитов ИБ;
− самооценок ИБ;
− мониторинга СОИБ и контроля защитных мер;
− анализа функционирования СОИБ;
− обработки инцидентов ИБ;
− выявления новых угроз и уязвимостей ИБ;
− оценки рисков;
− анализа перечня защитных мер, возможных для применения;
− стратегических улучшений СОИБ;
− анализа СОИБ со стороны руководства;
− анализа успешных практик в области ИБ (собственных или других организаций).

9.14.2. Решения по тактическим улучшениям СОИБ должны быть документально зафиксированы и содержать либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо должны быть указаны направления тактических улучшений СОИБ в виде корректирующих или превентивных действий, например:
− пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
− пересмотр процедур эксплуатации отдельных видов защитных мер;
− пересмотр процедур обнаружения и обработки инцидентов;
− уточнение описи информационных активов;
− пересмотр программы обучения и повышения осведомленности персонала;
− пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
− пересмотр планов обработки рисков;
− вынесение санкций в отношении персонала;
− пересмотр процедур мониторинга СОИБ и контроля защитных мер;
− пересмотр программ аудитов;
− корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
− ввод новых или замена используемых защитных мер.

9.14.3. Вся деятельность по реализации тактических улучшений должна документально регистрироваться.

Программы реализации тактических улучшений СОИБ формулируются в представляемых на утверждение руководству планах.

Результаты выполнения указанных Планов фиксируются в отчетах СА.

9.14.4. Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться администратором ИБ.

9.14.5. Процедура согласования планов СА о тактических улучшениях СОИБ, об изменениях,

относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также отчетов, в которых документально зафиксированы результаты выполнения указанных процедур, заключается в утверждении указанных документов руководством.

После утверждения руководством о содержании указанных документов информируются заинтересованные лица в порядке, установленном порядком работы с документами, содержащими сведения ограниченного распространения».

9.14.6. В случаях принятия решений по тактическим улучшениям СОИБ должны быть назначены ответственные за их реализацию.

9.14.7. Руководство Организации осуществляет все необходимые организационные и тактические меры по обеспечению Организации необходимыми финансовыми, трудовыми и техническими ресурсами для реализации требований настоящей Политики.

РАЗДЕЛ 9.15. ТРЕБОВАНИЯ К ПРИНЯТИЮ РЕШЕНИЙ ПО СТРАТЕГИЧЕСКИМ УЛУЧШЕНИЯМ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.15.1. Для принятия решений, связанных со стратегическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых информационных активов Организации или их типов;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций);
- а также изменения:
- в законодательстве Российской Федерации;
- в нормативных актах Банка России, в частности, требованиях стандартов;
- интересов, целей и задач бизнеса;
- контрактных обязательств Организации.

9.15.2. Решения по стратегическим улучшениям СОИБ должны быть документально зафиксированы и содержать либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо указывать направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например:

- уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ;
- изменение в области действия СОИБ;
- уточнение описи типов информационных активов;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

9.15.3. Вся деятельность по реализации стратегических улучшений должна документально регистрироваться.

Программы реализации стратегических улучшений СОИБ содержатся в Планах, подготовленных СА и утвержденных руководством Организации.

Результаты выполнения указанных планов фиксируются в отчетах СА о реализации стратегических улучшений СОИБ, утвержденных Руководителем Организации.

9.15.4. Деятельность, связанная с реализацией стратегических улучшений СОИБ, должна быть санкционирована и контролироваться руководством Организации.

9.15.5. В случае стратегических улучшений СОИБ должна быть выполнена деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов. В частности, необходимо выполнить:

- выработку планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;

− уточнение процедур использования защитных мер.

9.15.6. Процедура согласования планов СА о стратегических улучшениях СОИБ, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также отчетов, в которых документально зафиксированы результаты выполнения указанных процедур, заключается в утверждении указанных документов руководством Организации.

После утверждения руководством Организации, о содержании указанных документов информируются заинтересованные лица в порядке, установленном порядком работы с документами, содержащими сведения ограниченного распространения.

9.15.7. В случаях принятия решений по стратегическим улучшениям СОИБ должны быть назначены ответственные за их реализацию.

РАЗДЕЛ 9.16. ПРОВЕРКА И ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

9.16.1. Проверка и оценка ИБ проводится путем выполнения следующих процессов:

− мониторинга и контроля защитных мер;
− самооценки ИБ;
− аудита ИБ;
− анализа функционирования СОИБ (в том числе со стороны руководства Организации).

Указанные процессы являются частью группы процессов «проверка» СМИБ, требования к которым приведены в Главе 4 настоящей Политики.

9.16.2. Основными целями мониторинга и контроля защитных мер в Организации являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели. Такими целями анализа могут быть:

− контроль за реализацией положений внутренних документов по обеспечению ИБ в Организации;
− выявление нештатных, в том числе злоумышленных, действий в АС;
− выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится персоналом, ответственным за ИБ.

Требования к проведению мониторинга и контроля защитных мер в Организации определены в подразделе 6.12 настоящей Политики.

9.16.3. При подготовке к аудиту ИБ рекомендуется проведение самооценки ИБ. Самооценка ИБ проводится собственными силами и по инициативе руководства Организации.

В процессе самооценки ИБ проводятся оценка степени выполнения требований настоящей Политики и на ее основе вычисление итогового уровня ИБ. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется Банком России.

9.16.4. Аудит ИБ, проводимый внешними по отношению к независимыми проверяющими организациями, является одной из форм проверки и оценки (контроля) выполнения Организацией требований настоящей Политики.

Аудит ИБ проводится как для собственных целей Организации, так и с целью повышения доверия к нему со стороны других организаций.

Аудит ИБ проводится в соответствии с требованиями стандартов Банка России.

В процессе аудита ИБ проводятся оценка степени выполнения требований стандартов Банка России и на ее основе вычисление итогового уровня ИБ. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется стандартом Банка России.

В качестве проверяющих организаций рекомендуется привлекать организации, имеющие квалификацию и опыт проведения оценки соответствия ИБ требованиям настоящего стандарта.

9.16.5. Анализ функционирования СОИБ проводится персоналом, ответственным за обеспечение ИБ, а также руководством, в том числе на основании подготовленных для руководства документов (данных).

Основными целями проведения анализа функционирования СОИБ являются:

− оценка эффективности СОИБ;
− оценка соответствия СОИБ требованиям законодательства Российской Федерации и стандартов Банка России;
− оценка соответствия СОИБ существующим и возможным угрозам ИБ;
− оценка следования принципам ИБ и выполнения требований по обеспечению ИБ, закрепленным в политике ИБ, а также в иных внутренних документах.

Результаты, полученные в ходе анализа функционирования СОИБ, являются среди прочего

основой для совершенствования СОИБ.

РАЗДЕЛ 10. ПОРЯДОК ВЫДЕЛЕНИЯ НЕОБХОДИМЫХ И ДОСТАТОЧНЫХ РЕСУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРИМЕНЕНИИ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР, ВХОДЯЩИХ В СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ

10.1. Все запросы, связанные с наличием необходимости приобретения нового программного обеспечения, техники, увеличением количества работников, задействованных в СОИБ, работники Организации доводит до сведения СА и/или руководства Организации.

10.2. По итогам анализа представленных работниками Организации запросов, СА формирует заявку руководству Организации на выделение соответствующих финансовых, технических либо трудовых ресурсов.

10.3. В возможно короткие сроки руководство Организации согласует заявку, и изыскивает финансовые, технические и трудовые ресурсы и направляет их на осуществление мер, входящих в систему защиты информации.

При этом все действия персонала, связанные с приобретением, распределением и внедрением ресурсов, оформляются распорядительной документацией по Организации.

РАЗДЕЛ11. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

11.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ в Организации при наличии стандартного уровня защиты информации назначается администратор ИБ, приказом по Организации утверждены цели и задачи его деятельности.

При отсутствии необходимости назначения администратора ИБ (при уровне защиты информации не выше минимального в соответствии с требованиями законодательства, функции администратора ИБ возложены на СА.

11.2. Служба ИБ наделена следующими полномочиями:

- организовывать составление и контролировать выполнение всех планов по обеспечению ИБ;
- разрабатывать и вносить предложения по изменению политик ИБ;
- организовывать изменение существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ;
- определять требования к мерам обеспечения ИБ;
- контролировать работников в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- осуществлять мониторинг событий, связанных с обеспечением ИБ;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ;
- участвовать в действиях по восстановлению работоспособности АС после сбоев и аварий;
- участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ.

Приложения:

- Приложение № 1 Инструкция по проведению антивирусного контроля (антивирусной защите) в ООО МКК «Экофинанс»;
- Приложение № 2 Процедуры мониторинга и анализа в ООО МКК «Экофинанс» данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции;
- Приложение № 3 Процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий;
- Приложение № 4 Порядок обеспечения готовности системных и прикладных программных и технических средств в ООО МКК «Экофинанс»;
- Приложение № 5 Порядок администрирования средств ИБ в ООО МКК «Экофинанс».

Приложение № 1
к Политике информационной безопасности
ООО МКК «Экофинанс»

Инструкция
по проведению антивирусного контроля (антивирусной защите)
в ООО МКК «Экофинанс»

1. Настоящая Инструкция содержит требования по обеспечению антивирусной защиты в ООО МКК «Экофинанс» (далее «Организация»).

2. С целью защиты информационных автоматизированных систем (далее АС) от вредоносных программ в Организации должны применяться только официально приобретенные средства антивирусной защиты. Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АС должны осуществляться СА. В целях обеспечения антивирусной защиты на АС производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на ответственного за защиту информации СА.

4. К применению на (АС) допускаются только лицензионные антивирусные средства.

5. Пользователи АС при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

Защита от вирусов состоит из нескольких этапов. На первом этапе выполняются регулярные профилактические работы согласно настоящей Инструкции. На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления. И на третьем этапе выполняется уничтожение вируса (вирусов) из ПЭВМ.

6. Ответственный за защиту информации АС совместно с администратором безопасности информации осуществляют периодическое обновление антивирусных пакетов и осуществляют контроль их работоспособности, обеспечивают невозможность самовольного, либо несанкционированного отключения средств антивирусной защиты. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

7. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.

8. Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

9. Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в Организации должны контролироваться СА.

10. Требования к подсистеме анализа защищенности информационных систем и ресурсов в Организации:

- незамедлительное выявление уязвимостей на основе имеющихся в базе данных сигнатур;
- реализация регламента сканирования, включающего периодичность сканирования, использование правил и параметров сканирования, режимов;
- обеспечение подробных рекомендаций по устранению найденных уязвимостей;
- формирование оценки степени их критичности выявленных уязвимостей

11. Требования к подсистеме обнаружения несанкционированной активности:

- обнаружение несанкционированной активности на сетевом, системном и прикладном уровнях;

− обнаружение атак на информационные ресурсы на основе сравнения текущего состояния систем (сетевой активности, системных и прикладных журналов аудита и др.) с сигнатурами атак;

− возможность прекращения несанкционированной активности;

− регистрация зафиксированных несанкционированных действий, в том числе даты и времени событий, типа событий, идентификатора субъекта, приоритета события;

− удаленное обновление базы данных сигнатур атак;

− обеспечение доступа к базе данных зафиксированных событий, включая возможность поиска, сортировки, упорядочения записей протоколов, основанный на заданных критериях;

− обеспечение уведомления администратора о фактах несанкционированной сетевой активности (локально и удаленно);

− разграничение прав доступа работников - пользователей и администраторов к различным компонентам системы.

12. Требования к подсистеме управления информационной безопасностью:

− обеспечение контроля порядок организации и выполнения работ по защите информации;

− определение должностных обязанностей, прав и степени ответственности СА (в соответствии с должностными инструкциями);

− соблюдение порядка физической защиты технических средств.

13. Требование по контролю за наличием в программном обеспечении “закладок” и “троянских коней”, “задних дверей”:

обеспечение превентивных мер:

− контроль целостности системы;

− проверка благонадежности программистов-разработчиков;

− организация надлежащего хранения и контроля допуска к исходным текстам программ, средствам программирования и отладки;

− проведение опытной эксплуатации;

− постоянный антивирусный контроль;

− использование сканеров безопасности;

− закрытие лишних портов;

− анализ журналов регистрации;

− контроль атаки программных вирусов

Превентивные меры:

− создание закрытой среды функционирования ПО системы;

− контроль целостности ПО;

− контроль наличия в ПО неизвестных программ;

− контроль доступа к системе;

− регулярное тестирование ПО антивирусными программами;

− использование лицензионного программного обеспечения;

Восстановительные меры:

− наличие дистрибутивов системного ПО для восстановления системы;

− наличие резервных копий информационного обеспечения системы для восстановления;

14. Наиболее характерные внешние проявления вирусов

1) Вирус представляет собой программу, которая разрушает информацию на магнитных носителях или нарушает работу ПЭВМ, а также обладает способностью к размножению, т.е. вирус может самостоятельно внедряться в другие программы, переносить себя на диски и дискеты, передаваться локальной компьютерной сети.

2) Можно выделить несколько видов воздействия вирусов на ПЭВМ:

− вирусы разрушительного действия;

− вирусы, замедляющие работу ПЭВМ;

− вирусы рекламного характера;

− вирусы-шутки.

3) Самые опасные вирусы это вирусы разрушительного действия. Наиболее характерные внешние проявления вирусов этого вида:

− осыпание различных символов с экрана;

− появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;

− самопроизвольная перезагрузка операционной системы;

− зависание компьютера;

− появление неисправных участков (кластеров) на «винчестере»;

− неожиданные действия рабочих программ (не предусмотренные документацией на программы);

− искажения данных в обрабатываемых файлах.

4) Вирусы, замедляющие работу ПЭВМ, проявляют себя тем, что работа процессора замедляется в 3040 раз.

5) Вирусы рекламного характера и вирусышутки хотя и не портят информацию в ПЭВМ, однако замедляют работу или навязывают пользователю ненужные диалоги, что также замедляет весь процесс решения задачи.

6) Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.

7) Некоторые внешние неожиданные отклонения в работе ПЭВМ, описанные выше, не обязательно являются следствием наличия вирусов. Так, появление неисправных кластеров на «винчестере» может быть вызвано действительно неисправностью устройства, что определяется анализом ситуации.

15. Профилактика вирусов

1) Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в ПЭВМ. Поэтому целесообразно включать эти работы в планы работ подразделений. К основным профилактическим работам и мероприятиям относятся:

− ежедневная автоматическая проверка наличия вирусов при включении ПЭВМ;

− регулярная (не реже одного раза в месяц) комплексная проверка наличия вирусов во всех ПЭВМ, даже при отсутствии внешних проявлений вирусов;

− проверка наличия вирусов в ПЭВМ, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;

− изучение информации по сообщениям в компьютерных журналах и газетах о новых вирусах;

− создание резервной копии программного продукта сразу же после приобретения;

− тщательная проверка всех поступающих и купленных программ и баз данных; проверку необходимо выполнять либо на ПЭВМ без «винчестера», либо на отдельно выделенной ПЭВМ, не входящей в локальную сеть;

− ограничение доступа к ПЭВМ посторонних лиц.

2) Для ежедневной автоматической проверки наличия вирусов при включении ПЭВМ необходимо включить в файл запуска работы компьютера команду запуска антивирусной программы ревизора. Это включение выполняет СА.

3) Регулярную комплексную проверку наличия вирусов выполняет СА, который использует для проверки специальные антивирусные программы.

4) При обнаружении вирусов в ПЭВМ, работающей в локальной сети, проверке подлежат все ПЭВМ, включенные в эту сеть.

5) Создание резервной копии программного продукта выполняет СА, ответственный за внедрение этого программного продукта.

6) Проверку всех поступающих и купленных программ выполняет управление информатизации.

16. Анализ ситуаций.

1) Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов в ПЭВМ, то прежде всего необходимо убедиться в действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера.

Также появление сообщений антивирусных программ может быть вызвано разрушением.

2) Анализ ситуации наличия вирусов или неисправности какого-либо устройства ПЭВМ выполняет администратор ИБ. При анализе могут использоваться специальные программы проверки исправности ПЭВМ. В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости ремонта ПЭВМ.

3) Если вирус проник в ПЭВМ с автономных носителей, то необходимо определить источник, проверить на наличие вирусов ПЭВМ. Если источник носителя коммерческая или другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

В случае действительного наличия вирусов привлекается СА для проведения служебного расследования.

4) Ответственный за обеспечение защиты информации проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

5) По факту выявления вирусов проводится служебное расследование специалистами подразделения информатизации.

При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность СА и прекратить какие-либо действия на АС.

В случае обнаружения компьютерных вирусов:

− предпринимаются необходимые меры по отражению и устранению последствий вирусной атаки;

− в исключительных случаях угрозы безопасности информации СА уведомляет руководство;

по решению руководства при наличии угрозы ИБ производится приостановление работы (на период устранения последствий вирусной атаки).

17. СА производит ежемесячный контроль за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АС.

18. СА проводит, в случае необходимости, «лечение» зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

Процедуры мониторинга и анализа в ООО МКК «Экофинанс» данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции

Для проведения процедур мониторинга и анализа данных регистрации, действий и операций используются специализированные программные и (или) технические средства.

Комплекс мер по обеспечению информационной безопасности платежного технологического процесса включает:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов;
- минимально необходимый, гарантированный доступ работника только к тем ресурсам технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения информации;
- аутентификацию обрабатываемой информации;
- двустороннюю аутентификацию автоматизированных рабочих мест, участников обмена информацией;
- возможность ввода информации в АС только для авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- доставку электронных платежных сообщений участникам обмена;
- при эксплуатации системы дистанционного взаимодействия выполняются процедуры, реализующие в том числе механизмы:
- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными пользователями;
- доведения информации о возможных рисках, связанных с выполнением операций или транзакций до пользователей.
- Пользователи системы дистанционного взаимодействия обеспечены детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

В Организации неплатежная информация классифицируется как:

- открытая информация, предназначенная для официальной передачи во внешние организации и средства массовой информации;
- внутренняя информация, предназначенная для использования исключительно работниками при выполнении ими своих служебных обязанностей;
- информация, содержащая сведения ограниченного распространения в соответствии с утвержденным Организацией Перечнем, подлежащая защите в соответствии с законодательством Российской Федерации (например коммерческая тайна, персональные данные работников и т.п.);

Каждому виду информации соответствует свой необходимый уровень защиты (свой набор требований по защите). Обязанности по администрированию средств защиты неплатежной информации возложены на СА.

Процедуры мониторинга и анализа должны использовать критерии выявления неправомерных

или подозрительных действий и операций. Указанные процедуры мониторинга и анализа должны применяться на регулярной основе еженедельно, ко всем выполненным операциям и транзакциям.

Указанные критерии классифицируются следующим образом:

1) Неисправность (отказ, сбой, ошибка) средств информатизации

Вследствие неисправности (краха, отказа, сбоя, ошибки, наличия специальных закладок) аппаратных и/или программных средств, коммуникационного оборудования, каналов связи и носителей информации могут быть недоступны или потеряны данные (базы данных, файлы и программы), необходимые для функционирования АС, её отдельных подсистем, функциональных задач и отдельных АРМ.

Используемые средства и процедуры восстановления программных и технических средств, данных, а также их организация могут быть неадекватными или недостаточно эффективными для оперативного восстановления работоспособности АС и ёё элементов.

2) Отказ средств безопасности информации

При функционировании АС должна постоянно находится в безопасном состоянии, при котором правильно функционируют все средства сохранности и защиты информации. Такое безопасное состояние должно восстанавливаться в случае сбоя системы (отказа питания, краха, аварийного останова) или прерывания обслуживания.

Отказ (крах) системы может вызвать неадекватные механизмы восстановления при загрузке системы. Программы и объекты данных (базы данных) пользователей и регистрационная информация в системных журналах (аудита) могут быть изменены или потеряны при крахе системы вследствие разнообразных причин. При этом может быть также повреждено системное и прикладное программное обеспечение, включая данные средств безопасности информации.

3) Отсутствие проверки правильного функционирования технических и программных средств, целостности баз данных (файлов) АС и отсутствие адекватной организации их восстановления.

Несвоевременное выявление неправильного функционирования технических и программных средств, нарушение целостности и актуальности баз данных (файлов) по различным причинам при отсутствии оперативной адекватной реакции на такие события может вызвать нарушение функционирования АС.

4) Отсутствие проверки целостности программных средств при доставке и установке.

Системные и прикладные программные средства могут быть доставлены и установлены без предварительной проверки их работоспособности и целостности, что может привести к неправильному функционированию АС, «вирусному» заражению, искажению и потере данных.

5) Отказ в доступе

АС является инструментом для совместного использования и передачи информации. Нарушение функциональности АС может произойти, когда система не может выполнить свои функции в приемлемое время. Нарушение функциональности может приводить к прерыванию выполнения одной или нескольких функций (служб, сервисов). Возможный отказ в доступе к системе и ее ресурсам может произойти вследствие множества причин, как внутреннего, так и внешнего характера. Нарушители могут вмешаться в управление ресурсами системы и блокировать доступ к ее ресурсам, особенно таким, как каналы связи, дисковое пространство, память и загрузка процессора.

Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

- отсутствие обнаружения необычных видов трафика (например, намеренного переполнения какими-либо несанкционированными пакетами, а также специальных пакетов, характеризующие атаки на систему);
- невозможность перенаправить или блокировать трафик, справиться с отказами оборудования и т.п.;
- конфигурация АС, допускающая полный отказ из-за сбоя в одной точке;
- несанкционированные изменения компонент оборудования (изменение адресов рабочих станций, модификация конфигурации маршрутизаторов и мультиплексоров и т.п.), а также неправильное обслуживание аппаратных средств АС;

− недостаточная физическая безопасность оборудования АС.

6) Несанкционированная модификация данных и программ

Так как в АС пользователи могут использовать общие данные и прикладные программы, то необходимо контролировать все изменения таких ресурсов. Несанкционированные модификации данных и программ происходят, когда производятся несанкционированные изменения (дополнения, удаления, корректировки) файлов и программ. Когда необнаруженные модификации данных существуют продолжительное время, то изменённые данные могут распространяться по всей сети, возможно приводя к искажению баз данных, результатов вычислений и других различных прикладных данных. Без выявления изменений программных средств всё программное обеспечение становится подозрительным, требуя тщательной проверки (и возможно переустановки) всего соответствующего системного и прикладного программного обеспечения. Изменения могут быть произведены в простых программах (например, в командных файлах на рабочих станциях), в программных утилитах, используемых в многопользовательских системах, в главных прикладных программах или других типах программных средств. Такие изменения могут быть произведены несанкционированными посторонними лицами, а также теми, кому разрешено проводить изменения программ (хотя изменения, которые они осуществляют не санкционированы). Подобные изменения могут фальсифицировать или копировать информацию в другие места, разрушать данные при их обработке или блокировать доступность системы или различных прикладных подсистем (служб).

Программные «вирусы» направлены, главным образом, на разрушение рабочих станций (ПЭВМ) и, в большинстве случаев, не разрушают сетевые серверы (хотя «вирусы» могут использовать серверы для заражения ПЭВМ рабочих станций).

Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

− разрешение на запись предоставлено пользователям, которым требуется для доступа только чтение;

− произведены необнаруженные изменения программ, включая внедрение в них дополнительного кода для создания программ типа «троянский конь»;

− отсутствие криптографических контрольных сумм чувствительных данных;

− использование такого механизма распределения привилегий, который предоставляет не требующиеся права на запись;

− отсутствие защиты от «вирусов» и средств их обнаружения.

7) Физические атаки на средства сохранности и защиты информации

Средства сохранности и защиты информации могут быть подвержены физическим атакам, которые нарушат безопасность системы.

Безопасность может гарантироваться только в том случае, когда сами средства сохранности и защиты информации защищены от прямых физических атак. Это в свою очередь предполагает наличие соответствующих средств физической защиты для предотвращения возможных атак нарушителей получения непосредственного доступа к средствам сохранности и защиты информации или платформе, на которой они функционируют.

8) Несанкционированный доступ к системе

Нарушитель, имеющий или не имеющий физический доступ к АС и ее рабочим станциям (терминалам), может пытаться получить логический доступ к системе (АРМ) от имени законного пользователя путем кражи или подбора идентификатора и пароля для входа в систему (АРМ) и выполнять операции с её информацией, не имея на это право.

АС может подвергаться физическим атакам. При этом предполагается, что физические средства охраны оперативно сигнализируют службе информационной безопасности о физическом присутствии нарушителей (посторонних) внутри контролируемой зоны (зон).

Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

− отсутствие или слабые методы идентификации и аутентификации;

− использование одних и тех же паролей для нескольких пользователей;

− плохая организация по ведению паролей или установка паролей, которые легко угадываются;

− использование общеизвестных «дыр» и неисправленных ошибок в системе;

− узлы сети, включающие локальный интерфейс в виде клавиатуры и дисплея (рабочие станции PC, серверы, коммуникационное оборудование), не защищены паролем от загрузки;

− небрежное использование физических замков на оборудовании (PC, серверах, маршрутизаторах и т.п.);

− хранение паролей доступа в командных файлах;

− отсутствие контроля доступа к сетевым устройствам;

− использование незащищённых модемов;

− отсутствие временной задержки при неправильной (несанкционированной) попытке входа;

− отсутствие разъединения соединения при многократных неправильных попытках входа и их регистрации;

− отсутствие извещения администратора информационной безопасности (сигнализации) и регистрации даты/времени последнего успешного и неуспешного входа в систему;

− отсутствие проверки подлинности пользователей в реальном масштабе времени (с целью обнаружения «маскарада»).

9) Несанкционированный доступ к коммуникационному оборудованию.

Нарушитель, имеющий или не имеющий физический доступ к конечному активному коммуникационному оборудованию системы (маршрутизатору, межсетевому экрану), может пытаться получить логический доступ к нему от имени законного администратора путем кражи или подбора идентификатора и пароля для выполнения административных функций, направленных на блокирование защитных функций, не имея на это право.

При этом предполагается, что физические средства охраны оперативно сигнализируют службе информационной безопасности о физическом присутствии нарушителей внутри контролируемой зоны, в которой размещается конечное коммуникационное оборудование.

Причины реализации данной угрозы аналогичны предыдущей угрозе.

10) Несанкционированный доступ к узлам локальной сети

Пользователи защищенных локальных сетей АС могут атаковать другие узлы (серверы, рабочие станции) своей сети (фрагмента, домена) с целью получения несанкционированного доступа к находящейся на них защищаемой информации.

11) Несанкционированный доступ к ресурсам системы

Нарушитель, имеющий логический доступ к системе, может пытаться получить доступ к ресурсам системы (защищаемой информации) и выполнить операции, на которые у него нет прав. Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

− использование установок привилегий для пользователей в системе по умолчанию, которые явно излишни для них;

− неправильное использование привилегий администратора (предоставление администраторских прав многим пользователям);

− данные либо вовсе не защищены (предоставлены всем), либо защищены недостаточно;

− отсутствие или неправильное использование механизмов по установке и проверке привилегий пользователей на доступ к данным;

− использование программно-аппаратных платформ рабочих станций (операционных систем), на которых отсутствует средства контроля доступа к файлам (без систем защиты информации от НСД).

12) Использование вспомогательных и излишних протоколов

Нарушитель может пытаться получить доступ к АС, используя вспомогательные сетевые и прикладные протоколы, пакетам которых разрешено проходить через коммуникационное оборудование, но которые не должны использоваться удаленными пользователями (абонентами) системы. В узлах ЛВС (серверах) могут устанавливаться (по умолчанию) прикладные сервисы, не используемые в системе, уязвимость которых может использовать нарушитель для получения несанкционированного доступа или блокирования работы узла.

13) Перехват и искажение информации во внешних каналах связи

Нарушитель может перехватывать и модифицировать (искажать) как конфиденциальную информацию, так и электронные документы АС, передаваемые по внешним каналам связи.

14) Подделка сетевого трафика

Данные, передаваемые по сети, не должны несанкционированным образом изменяться, как в результате плохой передачи в сети, так и нарушителями. Пользователи должны быть уверенными в том, что посланное ими сообщение получено без изменений. Модификация передаваемых данных может произойти вследствие преднамеренного или непреднамеренного изменения какой-либо части сообщения, включая содержательную и адресную информацию. Подделка сетевого трафика может включать 1) возможность принимать сообщения маскируясь под законный пункт назначения, или 2) маскируясь под законный источник сообщений, посылать сообщения куда либо. Для маскирования под принимающую станцию, необходимо, чтобы адрес пункта назначения выглядел бы как законный адрес принимающей станции. Перехват трафика может осуществляться прослушиванием сообщений, так как они передаются в широковещательном режиме всем станциям. Для маскирования под передающую станцию необходимо обмануть принимающего в том, что сообщение было законно отправлено с помощью подделки адреса источника или посредством «прокрутки» перехваченных сообщений. «Прокрутка» предполагает захват (запись) сеанса между отправителем и получателем и последующую повторную передачу ранее перехваченного сообщения (либо только заголовка сообщения с новым его содержанием, либо всего перехваченного сообщения).

Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

- передача сетевого трафика в явном (незашифрованном) виде;
- отсутствие отметки даты/времени, указывающей время отправки и время приёма;
- отсутствие механизма проверки подлинности сообщений или цифровой подписи;
- отсутствие контроля за программной средой РС;
- отсутствие механизма верификации сообщений в реальном масштабе времени (для использования против «прокрутки»).

15) Неправильная установка прав и привилегий пользователей

Определение и назначение администраторских и пользовательских прав может быть произведено таким образом, что защита системы будет нарушена вследствие нарушения полноты, целостности и непротиворечивости таблиц (матриц) разграничения доступа СЗИ.

В общем случае, права администраторов и пользователей могут быть сформированы неправильно, иметь ошибочные сочетания прав на выполняемые операции с объектами доступа (данными). Пользователям и администраторам также могут быть назначены права, которые не соответствуют их производственным обязанностям, предоставляя им либо излишние, либо слишком ограниченные полномочия.

Особая опасность проистекает из-за того, что администраторам предписываются конфликтующие права по отношению к принципу «разделения полномочий». Отдельному администратору может быть предоставлено право выполнения множества всех возможных операций над всеми защищаемыми объектами данных.

16) Отсутствие надзора за состоянием безопасности

Эта угроза относится к человеческому фактору, связанному с возможностью администратора или пользователя выявить события, влияющие на безопасность системы. Вследствие этого, система может использоваться в небезопасном режиме, который будет ошибочно представляться администратору или пользователю как безопасный. Проблема неизвещения о безопасности может проистекать от различных факторов. Например, возможно, что ошибки администратора или другие ошибки функционирования могут дезактивировать или отключить средства сохранности и защиты информации, может быть вызван крах системы, которая начнет снова функционировать в небезопасном режиме или система может быть установлена или сконфигурирована в незащищенное состояние.

17) Отсутствие оперативного обнаружения атак

Нарушитель может проводить повторяющиеся атаки на систему, а персонал АС не будет о них

оперативно извещен.

18) Отсутствие и недостатки регистрации

События, существенные с точки зрения безопасности информации, могут не фиксироваться в системном журнале (протоколироваться) или не быть однозначно связаны с пользователем, который их вызвал.

Управление и сопровождение средств сохранности и защиты информации АС зависит от возможности обнаружения и представления событий, связанных с безопасностью информации, от возможности определения ответственных за вызванные события, а также от защиты записей о таких событиях от несанкционированного доступа, модификации или уничтожения. Строгая персональная ответственность пользователей за свои действия и оперативное сообщение обо всех аномальных событиях является обязательным с точки зрения безопасности информации.

Если записи протоколирования не включают существенные с точки зрения безопасности информации события или недоступны, невозможно обнаружить атаки на систему. При этом невозможно также сопоставить записи с конкретными пользователями. В любом случае, невозможно адекватно отреагировать на атаки системы.

19) Отсутствие анализа системных журналов

Результаты системы регистрации (системные журналы) могут просматриваться и анализироваться недостаточно оперативно. Причиной такого положения может быть большой объем регистрируемых данных, так и отсутствие удобных средств просмотра и анализа таких данных. Кроме этого, возможно неправильное конфигурирование или отключение средств регистрации. В любом случае, нарушитель может избежать обнаружения своих повторяющихся попыток проникновения в систему и несанкционированных действий.

20) Отсутствие проверки целостности средств безопасности при доставке и установке

Средства сохранности и защиты информации (программно-аппаратное обеспечение) могут быть доставлены и установлены таким образом, что безопасность системы будет разрушена.

Информационная безопасность системы предполагает, что средства безопасности первоначально устанавливаются в безопасное состояние, т.е. правильно сконфигурированы и функционируют. Это, в свою очередь, включает наличие гарантий того, что такие средства доставлены именно в том виде, в котором производилась их оценка (сертификационная) и что они впоследствии правильно установлены.

21) Неправильное администрирование и функционирование средств безопасности

Нарушения безопасности могут быть вызваны неправильным администрированием или функционированием АС и средств сохранности и защиты информации.

22) Нарушение целостности и ошибки средств безопасности

Пользователи или нарушители посредством случайного обнаружения или намеренного исследования могут выявить недостатки и ошибки в средствах безопасности, которые были внесены при проектировании системы и которые могут ими использоваться для получения несанкционированного доступа.

Программы и данные, обеспечивающие безопасность системы, могут быть обойдены или скомпрометированы, вызвав нарушение целостности средств безопасности и их действенность в управлении защитой. В частности, может быть несанкционированно изменена конфигурация коммуникационного оборудования (межсетевого экрана) или модифицированы данные системы безопасности АС.

Подмена системы безопасности может произойти при доставке дистрибутива средств сохранности и защиты информации. Во время функционирования системы нарушители могут разработать методы нарушения целостности системы, вследствие чего средства безопасности можно будет обойти, модифицировать или отключить.

23) Отсутствие контроля эффективности средств безопасности

При эксплуатации средств сохранности и защиты информации необходимо периодически проводить контроль их эффективности. Средства сохранности и защиты информации со временем могут снижать свою эффективность, как вследствие неправильного сопровождения и обслуживания,

так и с появлением новых видов атак, которые используют уязвимости и слабые места системы безопасности.

Для информации, содержащей сведения конфиденциального характера, дополнительно учитываются перечисленные ниже угрозы.

24) Несанкционированная передача информации во внешние сети

Пользователи внутренних защищенных сетей АС, региональных площадок АС могут передать конфиденциальную информацию во внешние (посторонние) по отношению к системе сети.

25) Нарушение конфиденциальности данных

Данные, содержащие сведения конфиденциального характера и обрабатываемые в АС, требуют определённого уровня защиты. Утечка данных или программных средств, содержащих конфиденциальную информацию, может происходить в таких условиях, когда они доступны и предоставляются несанкционированным пользователям. Например, это возможно, когда ктолибо посторонний получает доступ к незашифрованным данным на рабочей станции и сервере, к экранам дисплеев и распечаткам на принтере. Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

- неправильные установки по управлению доступом, либо отсутствие управления доступом;
- отсутствие управления потоками информации;
- чувствительные данные, которые следует зашифровывать, хранятся в незашифрованном виде;
- исходные тексты программ хранятся в незашифрованном виде;
- мониторы дисплеев просматриваются в проходных помещениях;
- данные и архивные копии хранятся в общедоступных местах.

26) Перехват сетевого трафика

Перехват сетевого трафика происходит в том случае, когда несанкционированное лицо читает или получает каким-либо образом информацию, которая передаётся по сети АС. Сетевой трафик может быть скомпрометирован с помощью прослушивания или перехвата трафика, передаваемого по транспортной среде АС (например, с помощью подключения к сетевому кабелю, прослушивания эфира, неправильного использования предоставляемого сетевого соединения для подключения сетевых анализаторов и т.п.). Многие пользователи осознают важность обеспечения конфиденциальности информации, когда она хранится на их рабочих станциях или серверах, однако, также важно обеспечивать конфиденциальность информации, передаваемой по сети. Информация, которая может быть скомпрометирована таким образом, включает имена системы и пользователей, пароли, сообщения электронной почты, данные прикладных программ и т.п. Например, даже если пароли хранятся в системе в зашифрованном виде, они могут быть перехвачены в явном виде при их передаче от рабочей станции к файл-серверу. Файлы сообщений электронной почты, доступ к которым строго контролируется в системе, часто передаются по сети в явном виде и могут быть легко перехвачены.

Причинами реализации данной угрозы могут быть, в частности, следующие недостатки:

- недостаточная физическая защищённость сетевых устройств и среды передачи;
- отсутствие контроля за программной средой рабочих станций;
- передача данных в явном незашифрованном виде по среде передачи сети.

Указанные процедуры мониторинга и анализа должны применяться на регулярной основе, ежедневно, ко всем выполненным операциям и транзакциям.

Процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий

1. Идентификация объектов защиты информации выполняется путем указания их положения в структуре АС и определения их класса на основании классов объектов. Классификация объектов должна позволить устанавливать их взаимосвязи с полем угроз безопасности, вычленяя в процессе идентификации характерные наборы единичных угроз нарушения безопасности для каждого из классов АС.

В процессе идентификации объектов защиты (защищаемых ресурсов) может быть составлен перечень ресурсов, несанкционированный доступ к которым может привести к нарушению безопасности хранимых и обрабатываемых ресурсов.

Все подлежащие защите ресурсы должны быть категорированы по признаку доступности на открытые и конфиденциальные информационные ресурсы. Хранимая и обрабатываемая конфиденциальная информация критична к нарушениям целостности, доступности, конфиденциальности и подлинности. Открытая информация критична к нарушениям целостности, доступности.

Объекты защиты должны находиться под постоянным наблюдением СА, подлежать учету, аттестации.

Для обеспечения информационной безопасности при работе с ЭВМ в Организации функционирует система обеспечения прав доступа (парольная защита) электронных вычислительных машин. Идентификация, аутентификация и авторизация осуществляются штатными средствами операционной системы. Назначение/лишение полномочий по доступу работников к ресурсам ЭВМ и/или ЛВС санкционируется СА, несущими персональную ответственность за обеспечение информационной безопасности. Оперативный контроль доступа пользователей к ресурсам ЭВМ и/или ЛВС осуществляется СА. Данный журнал доступен для чтения, просмотра, анализа, хранения и резервного копирования только СА.

Для контроля управления доступом в Организации может быть обеспечено:

- выделение информации с ограниченным доступом, подлежащей защите на основе перечней сведений конфиденциального характера, разрабатываемых органами власти, на предприятиях и в организациях с учетом особенностей автоматизированной обработки информации, а также определение порядка отнесения информации к категории конфиденциальной;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации с ограниченным доступом;
- ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация с ограниченным доступом, непосредственно к самим средствам информатизации и коммуникациям;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- учет документов, информационных массивов, регистрация действий пользователей АС и обслуживающего персонала, контроль за санкционированным и несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;

− использование сертифицированных средств защиты информации при обработке конфиденциальной информации;

− использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

− физическая защита помещений и собственно технических средств АС с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей;

− криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных АС);

− исключение возможности визуального (в том числе, с использованием оптических средств наблюдения) просмотра обрабатываемой информации;

− предотвращение внедрения в автоматизированные системы программвирусов, программных закладок;

− использование волоконнооптических линий связи для передачи информации с ограниченным доступом;

− использование защищенных каналов связи;

− использование средств мониторинга событий ИБ и катострофо-устойчивости данных, функционирующих в составе инфраструктуры под управлением центра мониторинга и центра защищенного резервного хранения данных.

В составе АС применяются встроенные средства защиты информации от несанкционированного доступа. При распределении прав доступа персонала и клиентов к активам при помощи АС СА руководствуется спектром решаемых пользователем задач. Защита от несанкционированного доступа и разграничение прав пользователей в АС осуществляется путем присвоения уникальных логина и пароля каждому работнику, работающему с информационной системой. Доступ к системе без ввода корректного сочетания этих данных невозможен. Сотрудникам категорически запрещается передавать кому-либо свои логин и пароль.

2. Аутентификация пользователей

Проверка подлинности (аутентификация) пользователей при входе в операционную систему и прикладную подсистему должна проводится по идентификатору и паролю условно-постоянного действия.

2.1. Ведение аутентификационных данных пользователей

В системе должны использоваться удобные программные средства ведения аутентификационных данных пользователей (идентификаторов и паролей), включая их генерацию, просмотр и модификацию. Данные средства должны быть доступны только СА.

Санкционированным пользователям и администраторам может разрешаться модификация своих паролей в рамках установленных условий.

Средства безопасности должны обеспечивать защищенный механизм для изменения своих паролей самими пользователями. Такой механизм должен проводить повторную аутентификацию пользователей.

2.2. Защита аутентификационных данных пользователей

Средства безопасности должны обеспечивать защиту аутентификационных данных от несанкционированного просмотра, модификации и уничтожения.

Пароли (в электронном виде) следует хранить в преобразованном виде с помощью необратимого алгоритма.

2.3. Дополнительная защита аутентификационных данных пользователей

Средства безопасности должны автоматически подавлять или полностью обезличивать

представление в явном виде паролей на устройствах ввода/отображения.

2.4. Обработка отказов аутентификации

Средства безопасности должны обеспечивать полное выполнение процедуры аутентификации пользователя даже в случае ввода неправильного идентификатора. Сообщение об ошибке не должно содержать информации о том, какая часть аутентификационной информации (идентификатор или пароль) неправильная.

2.5. Отбор паролей

Средства безопасности должны включать механизм для проверки того, что пароли отвечают определенному качеству.

Пароли не должны повторно использоваться с тем же идентификатором пользователя в течение определенного времени. Если пользователи сами меняют пароли, то средства безопасности не должны извещать пользователя о том, что выбранный им пароль уже используется другим пользователем. Такие средства должны, по умолчанию, запрещать ввод паролей менее восьми символов в подсистемах, обрабатывающих конфиденциальную информацию.

Средства безопасности должны включать алгоритм для обеспечения выбора пароля, удовлетворяющего следующим условиям:

Длина пароля должна быть не меньше определенной в системе длины. Минимальная длина пароля по умолчанию должна быть равна 8 символам.

Алгоритм проверки сложности паролей должен быть изменяемым.

2.6. Генерация паролей

Алгоритмы генерации паролей, должны удовлетворять следующим требованиям:

Алгоритм должен генерировать пароли, которые легко запомнить.

Средства безопасности должны предоставлять альтернативный выбор пароля из сгенерированного перечня.

Пароли должны быть устойчивы к атакам прямого перебора.

Генерируемая последовательность паролей должна иметь случайный характер (последовательные значения не должны коррелироваться, а сами вырабатываемые последовательности должны скрывать свою периодичность).

2.7. Санкционирование по времени

2.8. Контроль доступа к параметрам доступа

Средства безопасности должны предоставлять средства отображения и модификации параметров доступа к системе только СА.

Средства безопасности должны предоставлять СА средства для отображения всех параметров доступа для отдельного пользователя, а также списка пользователей, связанных с определенным параметром доступа к системе.

2.9. Защищенный канал

Средства безопасности должны предоставлять канал связи между механизмами аутентификации и пользователями, который должен быть логически отличным от других каналов связи и обеспечивать гарантированную защищенную аутентификацию субъектов доступа.

Средства безопасности и пользователи должны иметь возможность инициировать связь через защищенный канал.

Средства безопасности должны требовать создание защищенного канала для первоначальной аутентификации пользователей и аутентификации других процессов, для которых требуется защищенный канал.

2.10. Привязка прав и привилегий пользователя к субъекту доступа

Средства безопасности должны однозначно связывать соответствующие права и привилегии пользователя с субъектами доступа (программами, процессами), инициированными пользователем. Такая связь должна быть защищена от какого-либо вмешательства.

2.11. Параметры управления доступом

Средства безопасности должны обеспечивать выполнение разрешительной системы доступа (правил безопасности) на основе прав и привилегий пользователей с учетом:

а) субъектов доступа (программ, процессов), выступающих от имени пользователей;

б) объектов доступа (данных), над которыми выполняются операции в соответствии с правами доступа;

в) операций, выполняемых над объектами в соответствии с заданными правилами.

Типы объектов доступа и допустимые над ними операции определяются для каждого программного продукта (операционной системы, СУБД, прикладной подсистемы).

2.12. Управление доступом на основе прав и разрешений

Субъект доступа (программа, процесс), функционирующий от имени пользователя, может выполнить операцию над объектом, если:

а) пользователь имеет право доступа к данному объекту, и

б) запрошенная операция предоставлена (разрешена) для данного пользователя, и

в) объект доступа разрешен для данной операции.

2.13. Дискреционное (избирательное) управление доступом

Средства безопасности должны обеспечивать избирательное (дискреционное) управление доступом к объектам на основе следующих атрибутов субъектов доступа:

а) идентификатора пользователя;

б) группы, к которой принадлежит пользователь.

Средства безопасности должны обеспечивать дискреционное управление доступом к объектам на основе следующих атрибутов объекта:

а) списка доступа: списка идентификаторов пользователей и/или списка групп, с указанием для каждого отдельного пользователя и члена группы списка разрешенных операций;

б) списка пользователей и/или списка групп, которым запрещен доступ к объекту.

Средства безопасности должны обеспечивать выполнение следующих правил для определения допустимости операции между контролируемыми субъектами и объектами:

Субъекту разрешается выполнение операции над объектом, если:

а) идентификатор пользователя соответствующего субъекта доступа не входит в список пользователей, которым запрещен доступ к объекту, и

б) идентификатор пользователя субъекта доступа входит в список доступа к объекту, или идентификатор пользователя входит в список групп доступа к объекту, и запрашиваемая операция содержится в списке разрешенных операций для данного пользователя (группы);

в) проверка списка (списков) разрешений на доступ к объекту не проводится, если пользователь входит в список пользователей, которым запрещён доступ к объекту.

2.14. Управление потоками информации

Для изолирования размещения данных, содержащих сведения конфиденциального характера, от других данных необходимо использовать следующие средства и методы управления потоками информации.

Изолирование сеанса для обработки конфиденциальной информации может выделяться для пользователей отдельный сеанс работы на АРМ и в ЛВС (с отдельным идентификатором и паролем), в котором будут доступны только те ресурсы, которые предназначены только для обработки и хранения конфиденциальной информации (серверы, АРМ, тома, каталоги, файлы и программы). В этом

случае, все возможные потоки информации строго определены и фиксированы.Введение строгого регламента для обработки конфиденциальной информации могут устанавливаться (организационно) строгие регламенты работы, определяющие те ресурсы АС (серверы, тома, каталоги, файлы, съёмные накопители), которые при этом могут использоваться. В таких регламентах должно чётко указываться, где может записываться и храниться информация ограниченного распространения.

Применение сертифицированных систем защиты информации от НСД, в которых имеются средства управления потоками информации на основе мандатного принципа разграничения доступом.

2.15. Санкционирование доступа и отказ в доступе

Средства безопасности должны обеспечивать дискреционное управление доступом для его предоставления или для отказа в доступе исключительно на основе значений указанных атрибутов субъектов и объектов.

2.16. Задание общих прав и привилегий пользователей по умолчанию

Средства безопасности должны обеспечивать создание (инициализацию) прав и привилегий пользователей по заданному умолчанию. Например, в рамках определенной группы пользователей создание нового члена группы влечет автоматическое предоставление ему общих прав и привилегий группы, в случае использования типовых ролей при создании пользователя ему приписываются определенные минимальные права и привилегии по умолчанию.

2.17. Ведение прав и привилегий пользователей

Средства безопасности должны предоставлять удобные программные средства для отображения и модификации прав и привилегий пользователей. Данные средства должны быть доступны только СА. Ни один администратор не должен иметь права ведения всех таких данных.

2.18. Установка индивидуальных прав и привилегий пользователей

Средства безопасности должны предоставлять СА возможность устанавливать индивидуальные права и привилегии для каждого пользователя.

2.19. Инициализация атрибутов

Средства безопасности при дискреционном управлении должны обеспечивать создание ограничительных значений атрибутов объектов доступа по умолчанию.

Средства безопасности должны позволять задавать альтернативные начальные атрибуты объекта доступа, заменяющие значения по умолчанию при создании объекта.

Средства безопасности должны предоставлять возможность для санкционированных пользователей изменять значения по умолчанию атрибутов доступа относящихся к ним объектов доступа (владельцами которых они являются).

2.20 Ограничение множества атрибутов

Средства безопасности должны ограничивать набор атрибутов безопасности (прав и привилегий) каждого сеанса на основе идентификатора пользователя.

Условия установления сеанса должны определяться только СА.

2.21. Изменение атрибутов

Средства безопасности при управлении доступом должны предоставлять администратору возможность изменять списки доступа к объектам, которые он создал.

2.22. Запрос атрибутов администратором

Средства безопасности при управлении доступом на основе групп, «ролей» (совокупностей типовых прав и привилегий, которые предоставляются отдельным пользователям или группам) должны предоставлять администратору средства для получения (просмотра) идентификационной и

аутентификационной информации, прав, привилегий и операций (атрибутов доступа), разрешенных пользователям групп и содержащиеся в «ролях» по отношению к объектам доступа.

2.23. Запрос атрибутов пользователем

Средства безопасности должны предоставлять санкционированным пользователям средства для получения (просмотра) следующих значений:

а) имен всех групп;

б) списков доступа тех объектов, владельцами которых они являются.

2.24. Максимальные квоты

Средства безопасности должны устанавливать квоты, ограничивающие максимальный размер (количество) контролируемых ресурсов (объем памяти), который могут использовать отдельные пользователи, группы пользователей одновременно или в течение определенного времени.

2.25. Регистрация при работе с электронными документами

Средства безопасности должны регистрировать следующие события:

а) запуск и остановку средств регистрации;

б) события, связанные с функциональными компонентами (средствами безопасности), а именно:

- любое использование программно-аппаратных средств аутентификации;
- принятие или отвержение любого вводимого пароля при аутентификации;
- отказ в создании нового сеанса с учетом ограничения на число одновременно устанавливаемых сеансов;
- все попытки установления сеансов пользователями;
- блокирование интерактивного сеанса механизмом его блокировки;
- успешное разблокирование интерактивного сеанса;
- окончание интерактивного сеанса механизмом его завершения;
- успешное применение предупредительных действий, которые должны использоваться при возможном нарушении безопасности;
- истечение срока действия атрибутов безопасности (паролей);
- разрешения на запрошенные операции;
- отказы на запрошенные операции;
- успешные и неуспешные попытки активизации (запуска) программ (процессов) субъектами доступа (пользователями);
- идентификатор пользователя или субъекта доступа неуспешно пытавшийся экспортировать (передать, переместить) объект доступа (файл);
- любые попытки выполнения операций с системным журналом, т.е. любые попытки чтения, изменения или уничтожения системного журнала;
- извещения СА в случае переполнения системного журнала.

Средства регистрации должны приписывать к каждой записи, по крайней мере, следующие данные:

а) дату и время возникновения события, тип события, идентификатор субъекта доступа и результат завершения события: успешное/неуспешное;

б) для каждого типа регистрируемого события с учетом специфики соответствующей функциональной компоненты другие характерные данные.

2.26. Регистрация при работе с конфиденциальной информацией

При работе с конфиденциальной информацией средства безопасности должны дополнительно регистрировать:

- любые попытки использования программных средств ведения аутентификационных данных (идентификаторов, паролей);

− все успешные и неуспешные (несанкционированные) попытки доступа к аутентификационным данным (идентификаторам, паролям);

− все попытки использования программных средств ведения атрибутов безопасности пользователей (прав, привилегий, разрешений, ограничений и т.п.);

− изменение атрибутов пользователей с указанием их значений;

− изменение параметров (условий и ограничений) аутентификации (изменение связи с определенными событиями даты, времени и т.п.);

− установка аутентификационного механизма (программы, сервиса);

− все попытки использования программных средств ведения идентификаторов пользователей, с регистрацией введенных идентификаторов;

− все попытки выбора атрибутов безопасности пользователей (паролей) из множества выбираемых атрибутов;

− идентификация инициатора и цель использования защищенного канала;

− все попытки использования функций защищенного канала;

− используемые атрибуты безопасности и идентификаторы пользователей, субъектов и/или объектов доступа при успешном их взаимодействии;

− идентификаторы пользователя и/или субъекта доступа успешно изменивший атрибуты безопасности объекта (список доступа) и идентификатор объекта, у которого проведена модификация;

− неуспешные попытки изменения атрибутов безопасности субъектов и объектов (пользователей и данных);

− новые значения измененных атрибутов;

− идентификаторы пользователя и/или субъекта доступа, неуспешно пытавшегося изменить атрибуты, объекта модификации, а также старые и запрашиваемые новые значения атрибутов;

− идентификаторы пользователя, успешно/неуспешно запросившего атрибуты безопасности объекта и объекта, у которого они запрашивались;

− включение и выключение любых механизмов выявления аномальных событий;

− извещения, выданные администратору механизмами выявления аномальных событий;

− автоматические ответные действия, выданные механизмами выявления аномальных событий;

− любые изменения конфигурации механизмов выявления аномальных событий;

− включение и выключение любых механизмов выявления проникновения;

− извещения, выданные администратору механизмами выявления проникновения;

− выявление нарушений механизмами надзора за безопасностью;

− все модификации конфигурации функций по регистрации событий во время работы;

− любое использование средств проверки целостности данных средств защиты;

− выявление модифицированных данных средств защиты;

− использование программных средств администратора информационной безопасности;

− введение новой функции (программ, сервиса) для администратора информационной безопасности.

− Другие регистрируемые события:

− использование и результат самотестирующих функций средств защиты;

− действия, предпринятые работниками - пользователями и администраторами системы и/или администраторами информационной безопасности;

− другие контролируемые события (при необходимости), для чего средства защиты должны иметь интерфейс для прикладных программ, позволяющий привилегированным прикладным программам добавлять записи в системный журнал или в отдельный журнал по безопасности прикладной программы.

Средства регистрации должны приписывать к каждой записи по крайней мере следующие данные:

а) дату и время возникновения события, тип события, идентификатор субъекта доступа и

результат завершения события: успешное/неуспешное;

б) для каждого типа регистрируемого события с учетом определения соответствующей функциональной компоненты другие специфические данные.

3. Авторизация пользователя

Средства безопасности должны однозначно связывать контролируемые события с индивидуальным идентификатором пользователя, который их вызвал.

3.1. Защита на уровне локальной сети, регистрация пользователей в сети.

Система безопасности доступа к сети определяет: какие пользователи могут работать на файловых серверах; в какие дни и в какое время пользователи могут работать, с каких рабочих станций пользователи могут работать.

Регистрация учётной записи пользователя на серверах локально–вычислительной сети (далее — «*ЛВС*») производится системным администратором на основании заявки, подписанной руководителем структурного подразделения работника.

Для контроля доступа к сети каждому пользователю присваивается один уникальный идентификатор (сетевое имя), который выдаётся ему системным администратором ЛВС при регистрации, и пароли для подключения к разным серверам. Срок действия пароля должен быть ограничен (как правило, не более 1 (одного) года).

При увольнении работника из, отстранении его от работы, изменении его служебных обязанностей и функций, его непосредственный руководитель обязан своевременно письменно известить об этом администратора ЛВС. Системный администратор обязан немедленно произвести соответствующие изменения в настройках учётной записи пользователя.

Каждому пользователю ЛВС при его регистрации устанавливается ограничение на количество соединений с каждым из серверов — как правило, даётся одно подключение к каждому из серверов, необходимых для работы пользователя. В качестве дополнительной защиты может использоваться привязка сетевых имён к MAC–адресам рабочих станций.

В случае необходимости временной передачи полномочий одного пользователя ЛВС другому руководитель соответствующего структурного подразделения обязан своевременно письменно известить об этом администратора ЛВС. При необходимости отмены делегирования полномочий администратор ЛВС также должен быть извещён. Не допускается передача сетевого имени и/или пароля от одного пользователя другому.

Заявки на подключение, делегирование полномочий и отключение (блокировку) пользователей к ресурсам сети хранятся бессрочно системным администратором.

Обо всех попытках несанкционированного доступа к информации в ЛВС системный администратор обязан немедленно сообщать Руководителю Организации. Системный администратор обязан иметь список пользователей, групп и структуру их доступа к сетевым ресурсам.

3.2. Разграничение доступа к ресурсам сети.

Разграничение прав доступа к определённым базам данных и программам, расположенным на файловых серверах, производится на уровне сетевых устройств и директорий. В случае использования серверных СУБД следует использовать их внутренние механизмы аутентификации пользователей и защиты данных.

Для организации совместной работы с ресурсами серверов и обмена данными через серверы создаются группы пользователей (например, по принципу административного деления, по используемым приложениям, каталогам и т.п.). Каждая группа имеет права доступа к определённым ресурсам. Права доступа групп, как правило, не пересекаются.

Каждый пользователь в соответствии с его функциональными обязанностями принадлежит к одной или нескольким группам пользователей.

На серверах должны отсутствовать имена общего пользования, такие как Guest. В случае наличия подобных имён по умолчанию после установки сетевой операционной системы подобные

учётные записи должны быть отключены. Беспарольный доступ к любым сетевым ресурсам запрещается.

Системный администратор обязан обеспечить минимальное наличие на рабочих станциях накопителей на сменных магнитных или оптических носителях. При отсутствии возможности физически снять подобного рода накопители с рабочих станций (наличие гарантийной пломбы и т.д.) системный администратор обязан отключить данные устройства встроенными средствами рабочей станции либо средствами операционной системы.

Несанкционированное использование пользователями съёмных носителей любого рода запрещается. Пользователи несут персональную ответственность за подобные действия. Доступ конкретных пользователей к подобным устройствам разрешается системным администратором после соответствующей обосновывающей заявки, подписанной руководителем структурного подразделения. Доступ посторонних лиц к съёмным носителям запрещён. Ответственность за доступ посторонних лиц к таким устройствам несёт пользователь, через рабочую станцию которого был произведён несанкционированный доступ.

Съёмные носители, содержащие информацию, имеющую отношение к деятельности, должны храниться в недоступном для посторонних лиц месте.

3.3. Разграничение прав доступа на уровне прикладных программ.

Для работы с системами каждый пользователь должен иметь свой уникальный идентификатор и пароль. В зависимости от выполняемых операций пользователю разрешается или предоставляется доступ к определённым компонентам системы (АРМам). При этом ограничивается доступ на уровне используемых функций и выполняемых операций. На самом низком уровне для исполнителей, работающих с операционным днём (далее — «ОДБ»), определяются группы доступных счетов и полномочия по работе с этими счетами.

Функции по определению прав доступа пользователей к прикладным системам возлагаются на СА.

3.4. Защита аппаратных средств.

Компьютерное оборудование должно располагаться в местах, которые исключают возможность доступа посторонних лиц без ведома работников. Основные серверы должны располагаться в отдельных комнатах, в которые имеет доступ СА.

Структура сети должна исключать несанкционированное подключение к магистрали или коммутирующим устройствам.

4. Сопровождение системного журнала

4.1. Средства безопасности должны включать средства администратора информационной безопасности для создания, удаления и очистки системного журнала.

Средства сопровождения системного журнала должны обеспечивать:

- архивирование файлов системных журналов на внешние накопители с одновременным их компрессированием;
- создание, уничтожение и очистку системных журналов;
- форматирование и компрессирование записей из системного журнала;
- отображение форматированных данных из системного журнала;
- автоматическое копирование файлов системных журналов во вспомогательную область памяти (каталоги файл-сервера, внешние накопители) после заданного для системы промежутка времени;
- автоматическое удаление файлов системного журнала после их архивирования;
- блокирование удаления системного журнала, если он не был предварительно сохранен во вспомогательной области памяти;
- поддержание целостности данных системного журнала после сбоев системы и прерывания ее работы.

.

4.2. Управление переполнением системного журнала

Средства безопасности должны вырабатывать сигнал для СА в случае превышения размера системного журнала заданных границ.

Средства безопасности должны предоставлять СА возможность определять граничные значения размера системного журнала, при достижении которых будет вырабатываться сигнализационное сообщение.

4.3. Доступ к системному журналу

Доступ к системному журналу для выполнения любых операций должен предоставляться только СА.

4.4. Анализ системного журнала

Средства безопасности должны включать и предоставлять средства для анализа данных системного журнала и для полного просмотра системного журнала только СА.

Средства безопасности должны предоставлять средства ограниченного просмотра системного журнала только для санкционированных пользователей.

4.5. Постоянное хранение системного журнала

Средства безопасности должны обеспечивать постоянное (архивное) хранение записей системного журнала на внешних носителях информации.

4.6. Предотвращение потерь данных системного журнала

Средства безопасности должны ограничивать число потерянных записей системного журнала вследствие сбоя системы, атаки на систему или переполнения памяти, выделенной для системного журнала.

В случае переполнения памяти, выделенной для системного журнала, такие средства должны по выбору либо игнорировать, либо предотвращать возникновение регистрируемых событий, за исключением вызванных СА.

5. Регистрация событий и действий, выборочная регистрация

Средства безопасности должны предоставлять возможность включать или исключать регистрацию событий на основе следующих атрибутов:

а) идентификаторов объектов, пользователей, субъектов доступа, АРМ и типа события;

б) списка дополнительных атрибутов, которые используются при регистрации.

5.1. Оперативный выбор регистрации

Средства безопасности должны предоставлять СА возможность выбора регистрируемых событий в любое время работы системы.

5.2. Оперативное отображение регистрируемых событий

Средства безопасности должны предоставлять только СА возможность просмотра типов регистрируемых событий во время работы системы.

6. Учёт носителей информации

В АС должен проводиться строгий учёт всех носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Маркировка носителей информации должна указывать их вид конфиденциальности (ДСП служебная тайна, КТ коммерческая тайна, ПД персональные данные и т.п.), принадлежность к подсистеме (административная, справочная и т.п.) и подразделению владельца ИСиР, в котором используется носитель, если учет ведется в каждом подразделении.

Хранение и использование съёмных носителей информации должно исключать

несанкционированный к ним доступ.

7. Защита остаточной информации

Средства безопасности перед выделением/освобождением ресурсов для всех объектов доступа (оперативной и внешней памяти), содержавших ранее конфиденциальные данные (информацию), должны обеспечивать недоступность ранее содержавшейся в них информации.

8. Шифрование информации

Данные электронных документов, передаваемые по сети телекоммуникаций АС, могут шифроваться перед передачей и/или защищаться от модификации электронной цифровой подписью (ЭЦП).

Должны использоваться только сертифицированные, либо разрешенные к использованию компетентными органами криптографические средства и средства ЭЦП. Использование таких средств должно осуществляться строго в соответствии с эксплуатационной документацией (правилами применения).

Порядок обеспечения готовности системных и прикладных программных и технических средств в ООО МКК «Экофинанс»

В АС должны регулярно проводиться процедуры проверки целостности при доставке и правильности функционирования любых программных и технических средств перед их установкой в системе в соответствии с рекомендациями, изложенными в инструкция и иных сопроводительных документах по установке (инсталляции) и обслуживанию указанных средств от их производителя (распространителя).

1. Контроль целостности программ

Средства безопасности должны включать средства (процедуры) для проверки целостности исполняемых программ АС. Проверка целостности программ может проводиться поразрядным сравнением с эталоном или по контрольным суммам. На случай выявления (обнаружения) нарушения целостности программ должны быть проведены процедуры восстановления целостности программ (переустановка, копирование с эталона) в соответствии с инструкциями и иными сопроводительными документами по установке (инсталляции) и обслуживанию указанных средств от их производителя (распространителя).

2. Тестирование вычислительных средств во время работы системы

Средства безопасности должны включать средства проверки правильности функционирования технических и программных средств АС.

Средства безопасности должны предоставлять возможность проверки целостности программ и данных (прикладных баз данных).

Средства безопасности должны выполнять набор само-тестирующих тестов во время начальной загрузки и периодически во время нормальной работы для проверки правильности функционирования технических и программных средств АС:

а) должны предусматриваться аппаратные и/или программные средства, которые могут использоваться для периодической проверки правильности функционирования программно-аппаратных элементов АС. Эти средства должны включать: тесты по включению питания, загружаемые тесты и тесты, запускаемые администратором;

б) тесты по включению питания должны проверять все основные компоненты элементов программно-аппаратных средств АС, включая устройства и каналы обмена памяти; каналы данных; шины; регистры процессора и управляющей логики; контроллеры дисков; коммуникационные порты; консоли системы и динамики. Такие тесты должны охватывать все компоненты, которые необходимы для прогонки загружаемых тестов и тестов, запускаемых СА;

в) загружаемые тесты должны охватывать: компоненты процессора (например, арифметическое и логическое устройства, арифметическое устройство с плавающей точкой, буферы декодирования команд, контроллеры прерываний, шина обмена регистров, буфер трансляции адреса, кэш память и контроллер шины обмена процессор-память); другие шины; контроллеры памяти; записываемую управляющую память для проведения тестирования целостности системы с удаленного рабочего места или по командам администратора;

г) запускаемые по командам СА тесты должны проводить серию однократных или повторяющихся тестов при одновременном протоколировании их результатов и, в случае обнаружения ошибки, использовать программы проверки целостности для определения и локализации ошибки. Проведение тестов должно быть доступно только СА.

3. Тестирование средств информационной безопасности во время работы

Средства безопасности должны предоставлять СА средства для проверки правильности их функционирования.

Средства безопасности должны выполнять комплекс само-тестирующих средств во время первоначальной загрузки системы и периодически (по запросу) во время работы системы для проверки правильности своего функционирования.

4. Полное тестирование средств безопасности

Должно проводиться периодическое (не реже одного раза в год) тестирование всех функций применяемых средств безопасности. Такое тестирование проводится с помощью тестов разработчика при их наличии и доступности, в противном случае, с помощью тестов, разрабатываемых СА с учётом специфики работы конкретного технологического участка АС.

5. Сохранение безопасного состояния при сбое

Средства безопасности должны обеспечивать сохранение безопасного состояния при своих сбоях.

6. Автоматическое восстановление

При сбоях и прерываниях в обслуживании средства безопасности должны обеспечивать возврат системы в безопасное состояние с использованием автоматических процедур.

Если автоматическое восстановление после сбоя или прерывания обслуживания невозможно, то такие средства должны переходить в профилактический режим, в котором обеспечивается возврат системы в безопасное состояние.

Средства безопасности должны предоставлять СА средства для восстановления программ и данных в непротиворечивое и безопасное состояние.

7. Защита от обхода средств безопасности

Средства безопасности должны обеспечивать строгое выполнение установленных правил по сохранности и защите и отрабатываться до разрешения выполнения любых связанных с безопасностью действий.

8. Изолирование домена средств безопасности

Средства безопасности должны выполняться в безопасном домене (узле, платформе, программной области памяти), защищенном от влияния и вмешательства со стороны других субъектов доступа.

Средства безопасности должны осуществлять разделение адресного пространства контролируемых субъектов доступа.

9. Устойчивость передаваемых данных средств безопасности

Средства безопасности должны обеспечивать надежное распознавание типов данных во время их передачи между механизмами защиты.

Приложение № 5
к Политике информационной безопасности
ООО МКК «Экофинанс»

Порядок администрирования средств ИБ в ООО МКК «Экофинанс»

1. Определение ролей по администрированию средств безопасности

Средства безопасности должны различать административные функции по безопасности (привилегированные) от других функций.

Набор административных функций по безопасности должен включать все функции, необходимые для установки, конфигурирования и управления такими средствами.

Административные функции по защите должны быть доступны только СА.

Средства безопасности должны различать множество пользователей, которым разрешено использовать административные функции, от множества всех пользователей системы.

Средства безопасности должны требовать специальный запрос для назначения административных прав и привилегий по безопасности какому-либо пользователю.

2. Управляющие функции по безопасности

Средства безопасности должны предоставлять СА средства для установки и изменения следующих параметров:

а) метода аутентификации для каждого правила защиты, если используется несколько методов;

б) условий установления сеанса для ограничения множества контролируемых атрибутов;

в) ограничений атрибутов для каждого пользователя при нескольких одновременных сеансах;

г) значения интервала времени неактивности пользователей по умолчанию;

д) предупреждающего сообщения при доступе к системе;

е) времени доступа, расположения (адреса) устройства доступа и метода доступа (условий доступа);

ж) параметров регистрации системного журнала;

з) предельного размера системного журнала;

и) других конфигурационных параметров.

Средства безопасности должны предоставлять СА выполнение следующих административных функций:

а) создание именованных групп;

б) удаление именованных групп;

в) включение пользователей в одну или несколько именованных групп;

г) назначение пользователям прав доступа;

д) другие административные функции.