РОСВОДОКАНАЛ
Приложение № 1 к Приказу
Генерального директора
ООО УК «РОСВОДОКАНАЛ»

от 25.04.2023 №ИР-УК-25/04/2023-01

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ООО УК «РОСВОДОКАНАЛ»

Москва, 2023 г.

Оглавление

1. Общие положения

1.1. Настоящий документ разработан в соответствии с положениями международных стандартов: ИСО/МЭК 27001:2013, исправление 2, Стандарты ИСО/МЭК 27000:2018, 27002:2013, BS 25999 (ISO 22301). Непрерывность бизнеса, COBIT5 Control Objectives for Information and related Technology, 5 Edition, а также с учетом накопленного опыта в сфере обеспечения безопасности информационных технологий.

1.2. Документ закрепляет рискоориентированный и процессоориентированный подходы к функционированию и совершенствованию системы обеспечения (менеджмента) информационной безопасности в Группе компаний «РОСВОДОКАНАЛ» и определяет:

- цели и задачи системы обеспечения информационной безопасности;
- основные принципы и общие требования по обеспечению информационной безопасности;
- организацию системы обеспечения информационной безопасности.

1.3. На основании данной политики разрабатываются частные инструктивные документы и регламенты, конкретизирующие требования информационной безопасности для конкретных автоматизированных систем и условий их эксплуатации.

2. Список терминов и определений

Группа компаний (Компания) – Юридические лица, входящие в состав Группы компаний «РОСВОДОКАНАЛ».

Информационная система – совокупность информации, содержащейся в базах данных и обеспечивающих ее обработку информационных технологий и технических средств.

Пользователь – сотрудник Группы компаний, имеющий доступ к информационным ресурсам и/или использующий ИТ услуги.

Информационный актив - различные виды информации (платежной, финансово-аналитической. служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей основную деятельность подразделений Группы компаний и представляющей ценность с точки зрения достижения поставленных целей.

Владелец информационного актива – подразделение Группы компаний, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного актива определяется на этапе создания соответствующих массивов данных.

Авторизации пользователя - предоставление доступа к информационному активу в соответствии с установленными правами.

Данные – различные виды информации, представленные в электронной форме.

Доступность информационных активов (availability) –свойство ИБ организации, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых

пользователю, и в то время, когда они ему необходимы.

Идентификация риска – процесс выявления и классификации рисков.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки информации, при котором обеспечивается уровень защиты информационных активов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

Инцидент информационной безопасности – вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

Конфиденциальность (confidenciality) – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Критичный информационный актив (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные операции – операции, связанные с повышенными рисками информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных активов.

Критичные уязвимости – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных систем, создающие повышенные риски информационной безопасности критичным информационным активам.

Риск – возможность возникновения у подразделений Группы компаний финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности подразделений Группы компаний, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Информационный риск (ИТ-риск, риск автоматизации процессов) - риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных систем Группы компаний.

Риск информационной безопасности – риск, являющийся составной частью ИТ-риска, возникающий вследствие наличия угроз безопасности информационным активам подразделений Группы компаний.

Система обеспечения (менеджмента) информационной безопасности – часть общей системы менеджмента Группы компаний, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Группы компаний. Включает структуру, политики, совокупность мероприятий, методов и средств, обеспечивающих требуемый уровень безопасности информационных активов участниками соответствующих процессов.

Угроза информационной безопасности – внешний или внутренний фактор, создающий риск информационной безопасности.

Целостность (integrity) – обеспечение точности и полноты информации и методов ее обработки.

3. Перечень сокращений

АС - Автоматизированная система
ИТ (IT) - Информационные технологии
ЛВС - Локальная вычислительная сеть
ПО - Программное обеспечение
СУБД - Система управления базами данных
ДИТ - Департамент информационных технологий ООО УК «РОСВОДОКАНАЛ».
ДБ - Департамент безопасности
ДВА - Департамент внутреннего аудита
ЭЦП - Электронно-цифровая подпись
AD (Active Directory) - («Активный каталог») LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT.

4. Цели и задачи системы обеспечения информационной безопасности

4.1. Цель системы обеспечения информационной безопасности - создание и постоянное соблюдение в подразделениях Группы компаний условий, при которых риски, связанные с нарушением безопасности информационных активов, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне.

4.2. Задачами системы обеспечения информационной безопасности являются:

- снижение рисков, связанных с использованием информационных технологий;
- своевременное выявление новых угроз;
- контроль состояния информационной безопасности на всех этапах жизненного цикла автоматизированных систем;
- минимизация потерь в подразделениях Группы компаний при возникновении угроз информационной безопасности;
- обеспечение операционной деятельности компании и безопасности информационных активов в подразделениях Группы при возникновении неблагоприятных событий (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.);
- оптимизация затрат на обеспечение информационной безопасности.

4.3. Процессы обеспечения информационной безопасности подразделений

Группы компаний являются составной и неотъемлемой частью процессов управления информационными технологиями и сопутствующими операционными рисками и осуществляются на основе циклической модели

4.4. Безопасность информационных активов оценивается и обеспечивается по каждому из следующих аспектов:

- доступность
- целостность
- конфиденциальность

При этом критерием оценки является вероятность, размер и последствия нанесения подразделению Группы компаний любого вида ущерба (невыполнение имеющихся перед государством, клиентами и партнерами обязательств, финансовые потери, потеря репутации и пр.).

4.5. Состояние информационной безопасности оказывает непосредственное влияние на операционные риски деятельности Группы компаний, в связи с чем, любой факт (инцидент) нарушения информационной безопасности рассматривается как существенное событие.

5. Основные принципы обеспечения информационной безопасности

5.1. В компании определяются следующие основные принципы обеспечения информационной безопасности:

5.1.1. Осведомленность о риске информационной безопасности.

Система обеспечения информационной безопасности затрагивает каждого сотрудника подразделения Группы компаний, использующего его информационные активы, и накладывают на него соответствующие обязанности и ограничения.

5.1.2. Персональная ответственность.

Ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.

5.1.3. Ограничение полномочий.

5.1.3.1. Минимальность полномочий

Любому сотруднику подразделений Группы компаний доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

5.1.4. Комплексность защиты.

Меры по обеспечению безопасности информационных активов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности.

5.1.5. Адекватность защиты.

Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности.

5.1.6. Эргономичность защиты.

Средства защиты должны быть максимально "прозрачными" и удобными для пользователей и администраторов автоматизированных систем.

5.1.7. Документированность.

Документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально.

5.1.8. Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности.

В подразделениях Группы компаний осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом изменений IT- среды, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

5.1.9. Пассивность контроля.

Применяемые инструментальные средства контроля и обеспечения информационной безопасности не предоставляют доступ сотрудникам, ответственным за их эксплуатацию, непосредственно к критичной информации.

5.1.10. Разделение полномочий по управлению ИТ.

В подразделениях Группы компаний реализована структура управления информационными технологиями, направленная на исключение конфликта интересов и строгое разграничение ответственности при обеспечении функционирования и безопасности информационных активов: разделены обязанности подразделений и сотрудников, осуществляющих администрирование коммуникационного оборудования, операционных систем, СУБД, автоматизированных систем, средств защиты, и осуществляющих функции мониторинга состояния информационной безопасности и контроля (аудита) выполнения требований информационной безопасности.

5.1.11. Контроль со стороны руководства.

Руководство ДИТ на регулярной основе рассматривает отчеты о состоянии информационной безопасности в подразделениях Группы компаний и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика информационной безопасности и предложения по ее актуализации рассматривается Генеральным директором ООО УК «РОСВОДОКАНАЛ» ежегодно.

5.1.12. Сочетание централизованного и децентрализованного подходов к управлению рисками информационной безопасности.

В Группе компаний «РОСВОДОКАНАЛ» сочетаются централизованный и децентрализованный подходы к обеспечению информационной безопасности. ООО УК «РОСВОДОКАНАЛ» разрабатывает нормативные, методические и инструктивные материалы по обеспечению информационной безопасности, определяет требования к используемым в подразделениях Группы компаний средствам обеспечения информационной безопасности и проводит единую техническую политику. Подразделения Группы компаний в соответствии с

утвержденными нормативными документами обеспечивают необходимый уровень информационной безопасности в подчиненных им подразделениях. При необходимости, подразделения на основе нормативных документов ООО УК «РОСВОДОКАНАЛ» могут разрабатывать частные инструктивные документы и регламенты, конкретизирующие требования информационной безопасности для конкретных автоматизированных систем и условий их эксплуатации.

5.1.13. Контроль использования интерфейсов ввода(вывода).

Меры по обеспечению информационных активов предусматривают контроль использования интерфейсов, разрешенных и (или) запрещенных к использованию в АС.

5.2. Реализация процедур оценки рисков информационной безопасности.

Учитывая, что наиболее трудоемким и субъективным процессом обеспечения информационной безопасности является оценка рисков, а также с учетом необходимости унификации и максимального удешевления технологий защиты, в Группе компаний «РОСВОДОКАНАЛ» осуществляется:

5.2.1. Категорирование информационных активов по степени их критичности;

Категорирование осуществляется подразделением - владельцем информационного актива по каждому из аспектов информационной безопасности: доступности, целостности и конфиденциальности.

5.2.2. Использование типовых требований безопасности, дифференцированных по категориям информационных активов.

Выполнение типовых требований обеспечивает соответствующий базовый уровень информационной безопасности для каждой категории информационных активов.

5.2.3. Использование типовых средств и процедур обеспечения информационной безопасности для разных информационных активов одной категории.

5.2.4. Использование единой модели злоумышленника, адекватной реальным угрозам.

5.2.5. Оценка достаточности базового уровня безопасности с учетом конкретных особенностей применяемых информационных технологий и связанных с ними угроз.

В случае недостаточности, по результатам проведенного анализа рисков, обеспечиваемого базового уровня безопасности осуществляется определение дополнительных требований и мер обеспечения информационной безопасности.

5.3. Модель угроз и нарушителей информационной безопасности.

Любое лицо, имеющее логический или физический доступ к информационным активам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи) может являться потенциальным злоумышленником. При этом предполагается возможность сговора

сотрудника подразделения Группы компаний с внешним злоумышленником, но не сговор двух и более сотрудников подразделений Группы компаний.

Целью злоумышленника является получение контроля над информационным активом, приводящего к нарушению его доступности, целостности или конфиденциальности.

Для достижения целей злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры информационных систем.

Источниками угроз информационным активам являются:

- Внешние и внутренние злоумышленники;
- Ошибочные действия персонала подразделений;
- Вирусные атаки;
- Отказы и сбои оборудования и программного обеспечения;
- Техногенные и природные катастрофы;
- Террористические угрозы.

6. Общие требования по обеспечению информационной безопасности

В основе процессов управления информационной безопасностью лежат следующие общие требования:

6.1. Управление ролями и обеспечение доверия к персоналу

6.1.1. "Ролевое" управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

6.1.2. Роли формируются с учетом принципа минимальности полномочий.

6.1.3. Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

6.1.4. Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

6.1.5. В критичных системах по решению владельца информационного актива может вводиться роль администратора информационной безопасности АС, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

6.1.6. Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по ФЗ № 152 «О персональных данных», обеспечению информационной безопасности, включая обязательства по неразглашению информации, составляющей коммерческую тайну.

6.1.7. Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным

нарушениям, доводятся до всех сотрудников подразделений Группы компаний под роспись.

6.1.8. Реализуются программы обучения и аттестации персонала подразделений Группы компаний и информирования в вопросах обеспечения информационной безопасности. Периодически проверяется и оценивается уровень компетентности персонала в этих вопросах.

6.1.9. При допуске к работе с критичными АС, а также периодически, сотрудники подразделений проходят проверку методами, разрешенными законами Российской Федерации.

6.1.10. Ролевое управление процессами обеспечения информационной безопасности в подразделениях Группы компаний отражено в разделе 7 настоящей Политики.

6.2. Управление доступом к информационным активам и регистрация.

Модель разграничения прав доступа используется для защиты информации в системе, осуществляется посредством предупреждения преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения; нарушения ее доступности и работоспособности технических средств.

6.2.1. Все информационные активы идентифицируются, категорируются и имеют своих владельцев.

6.2.2. Доступ сотрудников подразделений к информационным активам предоставляется только на основании документально оформленных заявок, согласованных с их владельцами (в электронном или бумажном виде). По умолчанию определяется отсутствие доступа.

6.2.3. Доступ к информационным активам не предоставляется (прекращается) в случаях: отсутствия (минования) производственной необходимости; изменения функциональных и должностных обязанностей; увольнения сотрудника; нарушение сотрудником положений политики информационной безопасности.

6.2.4. Проводится периодический (для наиболее критичных систем - не реже одного раза в год) контроль соответствия согласованных и реальных прав доступа к информационным активам текущему статусу пользователя.

6.2.5. Работа пользователей с базами данных осуществляется исключительно через экранные формы автоматизированных информационных систем. Прямой доступ пользователей к базам данных не предоставляется.

6.2.6. Доступ ко всем информационным активам осуществляется только после авторизации пользователя. Необходимо использовать процедуру сильной (не имеющей недостатков клавиатурных паролей) аутентификации при доступе к разным информационным активам. Разграничивается авторизация на уровне AD и АС. Построение авторизации на уровне AD имеет более высокий приоритет.

6.2.7. Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности. Глубина срока журнала аудита

указывается в паспорте информационного актива. Автоматизированные системы должны содержать штатные средства анализа аудит-файлов и формирования отчетов по заданным критериям.

6.2.8. Использование парольной защиты позволяет осуществлять контроль и управление доступом персонала к информационной системе, контроль и фиксацию событий, выявление и предупреждение неправомерного доступа.

6.2.9. Категории прав доступа

В системе определяется несколько видов прав доступа:

- Администраторский доступ 1-ого уровня с высокими привилегиями на заведение/блокировку и изменение прав доступа администраторов с меньшими привилегиями, имеет доступ к администрированию аппаратно-программных компонентов автоматизированных систем;
- Администраторский доступ 2-ого уровня, предназначенный для администрирования информационных систем, выполнения настроек и технических работ в системе;
- Технический доступ, предназначен для обмена данными между информационными системами;
- Пользовательский доступ, предназначенный для выполнения типовых операций в информационной системе.

6.2.10. Доступные методы аутентификации в автоматизированных системах.

Доступ к информационным активам производится только после авторизации, позволяющей однозначно идентифицировать субъект доступа (Личность пользователя).

Средства управления доступом должны быть защищены от модификации; не должно существовать путей обхода механизмов контроля доступа. Механизм управления доступом должен контролировать количество одновременно запущенных сессий работы с системой и иметь возможность их ограничения по количеству, запрета работы с различных сетевых адресов либо запрета работы с конкретных сетевых адресов.

Для обеспечения защиты критичных информационных активов должна применятся двух факторная авторизация Пользователя криптографическими методами аутентификации.

Защита информационных обменов между информационными системами, осуществляемых через публичную сеть «Интернет» должна осуществляться с использованием криптографических методов защиты.

Доступ к информационному активу без прохождения процедуры аутентификации является инцидентом информационной безопасности.

На АРМ со сменным графиком работы допускается использование групповых учетных записей. Групповые учетные записи должны иметь оформленное в установленном порядке разрешение на использование общих учетных записей с указанием ответственного.

Проверка актуальности прав доступа к автоматизированным системам должна осуществляться на регулярной основе не реже чем один раз в полгода.

Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Мобильные средства Пользователя, которые имеют доступ к информационным активам ГК «РОСВОДОКАНАЛ» должны быть зарегистрированы в реестре мобильных устройств.

Доступ к информационному активу с незарегистрированного мобильного средства является инцидентом информационной безопасности.

6.2.11. Реализация политики учета прав доступа

Для реализации политики разграничения доступа должна осуществляться регистрация действий по созданию, удалению и изменению свойств зарегистрированных субъектов доступа в разрезе:

- изменения полномочий субъектов доступа;
- создание, изменение и назначение ролей доступа;
- назначение и изменение прав доступа к объектам доступа.

6.2.12. В автоматизированной системе обеспечивается затемнение экрана средств вычислительной техники после 15 минут и блокирование сеанса доступа пользователя после 20 минут его бездействия(неактивности) или по запросу пользователя.

Блокирование сеанса доступа пользователя автоматизированной системы обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к АС (без выхода АС).

Блокирование сеанса осуществляется блокированием любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокировки сеанса.

Блокирование сеанса доступа пользователя в автоматизированной системе сохраняется до прохождения им повторной идентификации и аутентификации.

6.3. Управление жизненным циклом автоматизированных систем.

6.3.1. Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

6.3.2. Разработка, тестирование автоматизированных систем отделяются от эксплуатации:

- Разработчики программного обеспечения не допускаются к его промышленной эксплуатации.

- Разработка и тестирование программного обеспечения проводятся на

выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для промышленной эксплуатации автоматизированных систем. Хорошей практикой является выделение рабочих станций и серверов, предназначенных для разработки и тестирования программного обеспечения, в отдельный сегмент ЛВС, доступ из которого к промышленным системам ограничивается.

6.3.3. В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к финансовому ущербу, а также соблюдение условий конфиденциальности.

6.3.4. Системы сторонней разработки проверяются на соответствие требованиям информационной безопасности, предъявляемыми ДИТ УК «РОСВОДОКАНАЛ».

6.3.5. В состав документации на критичные автоматизированные системы в обязательном порядке входит документация по обеспечению ее информационной безопасности.

6.3.6. Для вновь устанавливаемых автоматизированных систем в эксплуатацию производится только после их оценки эффективности на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация АС, не прошедших оценку эффективности или имеющих не устранённые критичные замечания. Оценка эффективности проводится уполномоченной комиссией назначенной приказом руководителя организации, с обязательным участием сотрудника подразделения автоматизации и представителей подразделения ответственного за эксплуатацию данной АС.

6.3.7. При выводе АС из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

6.4. Антивирусная защита

6.4.1. Каждый сотрудник подразделения Группы компаний обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать службу информационных технологий при подозрениях на вирусное заражение.

6.4.2. Техническая возможность подключения пользователями к рабочим станциям ЛВС внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использование ГМД, CD-/DVD-дисководов максимально ограничивается.

6.4.3. Антивирусная защита обеспечивается использованием специализированного программного обеспечения.

6.4.4. Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств, контроль и

управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно в автоматизированном режиме. При этом обеспечивается минимально возможный период обновления с учетом обязательного предварительного тестирования на совместимость с системным и прикладным ПО.

6.4.5. При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных ресурсов и техническими возможностями такого обновления.

6.5. Использование ресурсов Интернет

6.5.1. Использование ресурсов Интернет в подразделениях Группы компаний разрешается исключительно в производственных целях.

6.5.2. Допускается использование канальных ресурсов сети Интернет для построения корпоративных сетей с обязательным использованием процедур шифрования трафика и защиты канала передачи данных.

6.5.3. Предоставление услуг клиентам Группы компаний и взаимодействие с партнерами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.

6.5.4. Подключение к рабочим станциям ЛВС мобильных телефонов, беспроводных (радио) интерфейсов, модемов и прочего оборудования, позволяющего выходить в Интернет, допускается только с согласования подразделения ИТ, установленным образом.

6.5.5. Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение сотрудниками Группы компаний на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства.

6.5.7. Доступ сотрудников к ресурсам сети Интернет санкционируется непосредственным руководителем и согласовывается с подразделением информационных технологий, которое осуществляет контроль за соблюдением сотрудниками требований информационной безопасности, включая контентный анализ сообщений.

6.5.8. На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия внешним атакам и распространению «спама».

6.5.9. Сотрудникам Группы компаний запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или

недееспособности.

6.5.10. Сотрудники Компании перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов. Порядок проверки должен быть определен в соответствующих локальных нормативных документах.

6.5.11. Допускается доступ в Интернет через сеть Компании для лиц, не являющихся сотрудниками Компании, включая членов семьи сотрудников Компании, в исключительных случаях и в строгом соответствии с установленным порядком (согласованная заявка на доступ). Доступ предоставляется через гостевой шлюз.

6.5.12. Специалисты подразделений информационных технологий имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.6. Использование корпоративной почты

6.6.1 Использование электронной почты в личных целях не допускается.

6.6.2 Запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

6.6.3 Работники Компании для обмена документами с контрагентами должны использовать только свой официальный адрес электронной почты.

Запрещается:

6.6.4 Рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

6.6.5 Рассылка рекламных материалов, не связанных с деятельностью Компании;

6.6.6 Подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

6.6.7 Поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

6.6.8 Пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

6.7. Использование средств криптографической защиты информации

6.7.1. Применение средств криптографической защиты информации для обеспечения безопасности информационных активов и взаимодействия с клиентами производится в соответствии с порядком, установленным государственными уполномоченными органами.

6.7.2. Использование средств ЭЦП обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при

взаимодействии с клиентами.

6.7.3. Использование иных аналогов собственноручной подписи (кодов аутентификации, PIN-кодов и пр.) при взаимодействии с клиентами допускается в технически и экономически обоснованных случаях.

6.7.4. Во внутренних системах подразделений Группы компаний электронная цифровая подпись и/или другие механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности, а также в случаях, когда необходимо строго разделить ответственность между подразделениями или сотрудниками.

6.7.5. Конфиденциальность информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования. В обоснованных случаях информация, составляющая коммерческую тайну, может также шифроваться при ее передаче в ЛВС и хранении на средствах вычислительной техники.

6.7.6. Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

6.7.7. Ключи электронной цифровой подписи, предназначенные для защиты финансового электронного документооборота с клиентами и сторонними организациями, изготавливаются сторонами самостоятельно.

6.8. Защита платежных и информационных технологических процессов

6.8.1. Технологические процессы должны быть максимально автоматизированы и обеспечивать возможность выполнения массовых и потенциально опасных операций без участия персонала за счет реализации эффективных процедур контентного контроля и защиты.

6.8.2. Выполнение критичных операций в ручном режиме ограничивается системой лимитов и ограничений.

6.8.3. Для защиты технологических процессов по результатам анализа рисков информационной безопасности применяются как штатные средства безопасности сетевых операционных систем, СУБД, так и дополнительные программные и программно-аппаратные комплексы и средства криптографической защиты, в совокупности обеспечивающие достаточный уровень безопасности на всех участках и этапах технологического процесса.

6.9. Обеспечение непрерывности бизнеса и восстановления после сбоев.

6.9.1. Непрерывность критичных бизнес-процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

6.9.2. Жизнедеятельность и безопасность информационных активов в условиях неблагоприятных событий, техногенных и природных катастроф обеспечивается созданием территориально удаленных Резервных Комплексов.

6.10. Обеспечение физической безопасности

6.10.1. Помещения подразделений Группы компаний категорируются в зависимости от критичности размещаемых в них информационных активов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации. Конкретные меры по технической укреплённости помещений, описываются в соответствующих локальных нормативных документах.

7. Организация системы обеспечения информационной безопасности

7.1. Общее руководство системой обеспечения информационной безопасности в Группе компаний «РОСВОДОКАНАЛ» осуществляют Генеральный директор и Правление.

7.2. Генеральный директор:

- утверждает и пересматривает политику информационной безопасности;
- организует процесс управления информационной безопасностью, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;
- обеспечивает условия и утверждает бюджет для эффективной реализации политики информационной безопасности;
- рассматривает информацию и отчеты о состоянии информационной безопасности.

7.3. Все подразделения группы компаний «РОСВОДОКАНАЛ» и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции:

7.3.1. Дирекция по безопасности

- участвуют в разработке стандартов, инструкций и иных нормативных документов в части информационной безопасности;
- совместно с Департаментом ИТ, участвуют в оценке рисков реализации угроз информационных активов;
- контролирует выполнение требований и процедур информационной безопасности при работе сотрудников с информационными активами;
- контролирует действия по восстановлению работоспособности информационных систем и ресурсов после сбоев и аварий.
- на основании информации полученной от ДИТ или иных источников в отношении инцидентов и фактов нарушений информационной безопасности по указанию Генерального директора, Директора по безопасности организует и проводит служебное расследование о результатах которого информирует ГД.

7.3.2. Департамент информационных технологий

- разрабатывает нормативные, инструктивные и методические документы по обеспечению информационной безопасности;
- разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;
- организует проведение единой антивирусной политики в группе компаний;
- обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;
- проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки.
- обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных систем;
- ведет Фонд программ и документации;
- осуществляет регистрацию инцидентов, имеющих отношение к информационной безопасности;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части автоматизированных систем.
- обеспечивает управление ключевыми системами средств криптографической защиты;
- эксплуатирует специализированные средства обеспечения безопасности информационных активов и обеспечивает соответствие характеристик данных средств необходимому подразделениям группы компаний уровню доступности;
- осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности, проводит расследования инцидентов и информирует ДБ и ДВА о результатах проведенного расследования;
- организует обучение персонала по вопросам информационной безопасности;

7.3.3. Дирекция по внутреннему аудиту

- В рамках своей деятельности осуществляет периодическую оценку надежности функционирования автоматизированных систем, включая контроль целостности баз данных и их защиты от несанкционированного доступа и (или) использования, наличие и эффективность планов действий на случай непредвиденных обстоятельств.

7.3.4. Подразделения Группы компаний

- проводят категорирование информационных активов, владельцами которых они являются, и определяют те из них, которые являются критичными;
- участвуют в оценке рисков реализации угроз их информационным

активам;

- устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными активами, владельцами которых они являются;
- разрабатывают нормативные и инструктивные документы с учетом требований информационной безопасности;
- обеспечивают выполнение требований и процедур информационной безопасности при работе сотрудников с информационными активами.

8. Ответственность за нарушение требований по обеспечению безопасности ИТ

8.1. Сотрудники подразделений Группы компаний, нарушающие требования политики ИБ, регламентов по обеспечению требований ИБ, приказов и распоряжений, а так же руководители подразделений, не обеспечивающие их выполнение, несут ответственность в соответствии с действующим трудовым законодательством <i1>.

8.2. К нарушителям могут применяться дисциплинарные взыскания: замечание; выговор; увольнение по соответствующим основаниям.

8.3. При подозрениях на мошенничество, другие преступления с использованием ИТ или наличии материального ущерба, явившегося следствием нарушения безопасности ИТ, материалы передаются в следственные органы.

8.4. Администраторы ИТ всех уровней должны быть ознакомлены с данной Политикой под роспись.

8.5. Сотрудники подразделений, в которых используются ИТ, должны быть ознакомлены с настоящей Политикой, регламентами в области обеспечения ИБ, руководством по применению паролей и выпиской из уголовного кодекса РФ под роспись.

8.6. Контроль за выполнением требований настоящей Политики информационной безопасности и регламентирующих документов по ИБ возлагается на руководителей соответствующих структурных подразделений.

9. Перечень используемых документов

9.1. ИСО/МЭК 27001:2013, исправление 2, официальное русское издание (ГОСТ Р, идентичный или модифицированный стандарт) отсутствует.

9.2. Стандарты ИСО/МЭК 27000:2018, 27002:2013.

9.3. BS 25999 (ISO 22301). Непрерывность бизнеса.

9.4. «Политика по управлению рисками в группе компаний «РОСВОДОКАНАЛ», ООО УК ««РОСВОДОКАНАЛ»», 2018, б/н

9.5. COBIT5 Control Objectives for Information and related Technology, 5 Edition.

---

[1] См. Трудовой кодекс РФ