

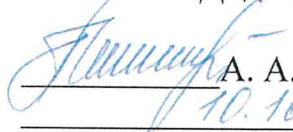
Политика

в области информационной безопасности ООО «Эн+ Диджитал»

Введен впервые

УТВЕРЖДАЮ

Генеральный директор
ООО «Эн+ Диджитал»

 А. А. Герасименко
10.10.2018
(дата)

Введен в действие приказом
ООО «Эн+ Диджитал»

от 08.10.18. № 23

ООО «Эн+ Диджитал»

Содержание

Содержание	2
Введение	3
1. Нормативные ссылки	3
2. Сокращения и определения	3
3. Общие положения	5
4. Цели и задачи	5
5. Объекты информатизации как объекты защиты	6
6. Основные факторы, влияющие на информационную безопасность	9
7. Основные принципы обеспечения информационной безопасности	9
8. Организация работ по защите информации	10
9. Ответственность сотрудников	12
10. Механизм реализации Политики	14
Лист регистрации изменений	15

Введение

Настоящая Политика определяет общие принципы и правила в области информационной безопасности в ООО «Эн+ Диджитал» (далее Компания).

Политика в области информационной безопасности Компании основана на российской и международной практике обеспечения информационной безопасности и консолидирует положения действующих отечественных и международных стандартов и требования законов РФ по вопросам обеспечения доступности, конфиденциальности, целостности информации, а также аутентичности и апеллируемости.

1. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.07.2004г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»;
- Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. ГОСТ Р ИСО/МЭК 27002-2012»;
- Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. ГОСТ Р ИСО/МЭК 27001-2006»;
- Международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;
- Международный стандарт ISO/IEC 27002:2013 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью»;
- Международный стандарт BS 7799-3:2006 RU «Системы управления информационной безопасностью – Руководство по управлению рисками информационной безопасности»;
- Национальный стандарт Российской Федерации «Защита информации. Основные термины и определения». ГОСТ Р 50922-2006.

2. Сокращения и определения

2.1. В настоящей политике используются следующие сокращения:

- ИБ** – информационная безопасность;
- СУИБ** – система управления информационной безопасностью;
- ИС** – информационная система;
- ИТ** – информационные технологии.

2.2. В настоящей политике используются следующие определения:

Владелец информационного ресурса – должностное лицо, исполняющее обязанности руководителя структурного подразделения, наделенное правами владения и ответственностью в отношении информационного ресурса в полном или ограниченном

объеме.

Владелец информационной системы – должностное лицо, исполняющее обязанности руководителя структурного подразделения, наделенное правами владения и ответственностью в отношении информационной системы в полном или ограниченном объеме.

Информатизация – это широкомасштабное применение методов и средств сбора, хранения и распространения информации, обеспечивающей систематизацию имеющихся и формирование новых знаний, и их использование Компанией для текущего управления, дальнейшего совершенствования и развития.

Информационная безопасность – состояние защищенности информации и информационных активов, при которых обеспечивается конфиденциальность, целостность и доступность информационных активов Компани, а также аутентичность данных и апеллируемость.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения бизнес задач подразделений Компании. В Компании используются различные типы информационных систем для решения производственных, управленческих, учетных и других бизнес задач.

Информационный актив – информация, хранящаяся на физических носителях (бумажные, магнитные, оптические и т.д.), а также информация в информационных системах и передаваемая по каналам связи; операционные системы; приложения; утилиты и т.д.

Информационный ресурс – информация в электронном виде, доступная посредством именованного раздела, в том числе прикладное и системное ПО, прикладные и системные данные.

ИТ служба – подразделение (работник) Общества, осуществляющее функции ИТ обеспечения Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

Компания – ООО «Эн+ Диджитал», а также партнеры, являющиеся пользователями или администраторами информационных систем ООО «Эн+ Диджитал», подписавшие соответствующие соглашения.

Локальная вычислительная сеть – группа персональных компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Модель угроз (безопасности информации) – Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Объект защиты – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с требованиями правовых документов или требованиями, установленными собственниками информации.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Подразделения ИБ – подразделение (работник), ответственное за контроль обеспечения ИБ Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

Угроза – совокупность условий и факторов, создающих потенциальную (но реализуемую фактически) или реально существующую опасность нарушения безопасности информации (например, связанную с утечкой информации, несанкционированными или

преднамеренными воздействиями на нее).

Уязвимость – брешь, свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

3. Общие положения

3.1. Настоящая Политика в области информационной безопасности:

3.1.1 строится в соответствии с Российским законодательством в области защиты информации, требованиями международных и отраслевых стандартов;

3.1.2 определяет основные цели и задачи, а также общую стратегию построения комплексной системы управления информационной безопасностью Компании, основные требования и базовые подходы к их реализации;

3.1.3 распространяется на все подразделения ООО «Эн+ Диджитал».

3.2. СУИБ представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов Компании от угроз безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных конкретными проектами, внутренними нормативными документами и стандартами безопасности, разрабатываемых на основе данной политики. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты.

3.3. Экономический эффект от внедрения СУИБ проявляется в снижении величины возможного ущерба, наносимого Компании, за счет мер, направленных на формирование и поддержание режима ИБ. Эти меры призваны обеспечить:

3.3.1 доступность информации (возможность за приемлемое время получить требуемую информационную услугу);

3.3.2 целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

3.3.3 конфиденциальность информации (защита от несанкционированного ознакомления);

3.3.4 неотказуемость (невозможность отказа от авторства);

3.3.5 аутентичность (подтверждение подлинности и достоверности электронных документов).

3.4. Политика ИБ Компании определяет подходы к определению состава критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты реализуемых при помощи СУИБ.

3.5. Перечень необходимых мер защиты информации определяется по результатам аудита информационной безопасности Компании и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения доступности информации и работоспособности технических средств, обрабатывающих эту информацию.

3.6. Политика пересматривается по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также производится по мере развития ИС Компании. Рекомендуемый срок пересмотра Политики составляет три года (при условии отсутствия коренных изменений в структуре системы, законодательстве, в технологиях управления и передачи информации).

4. Цели и задачи

4.1. Общие цели и задачи информационной безопасности – обеспечение бесперебойной работы Компании и сведения к минимуму ущерба от событий, несущих

угрозу безопасности, посредством их предотвращения и сведения к минимуму.

4.2. Цель настоящей Политики – создание и развитие системы управления информационной безопасностью за счет объявления стратегии защиты информационных ресурсов Компании и установления обязательных требований к поведению и практикам, связанным с информационной безопасностью.

4.3. При этом важнейшими задачами Компании в отношении информационной безопасности являются:

4.3.1. Планирование и реализация на всех этапах производства, обработки, передачи, хранения и получения информации мер ее достоверности, целостности, конфиденциальности и доступности, а именно:

- минимизация ущерба от событий (рисков) несущих угрозу информационной безопасности, посредством их предотвращения и/или сведения последствий таких событий (рисков) к минимуму;

- контроль состояния информационной безопасности на всех этапах производства, обработки, передачи, хранения и получения информации;

- установление четкой ответственности за управление и использование информационных ресурсов Компании;

- введение обоснованной, экономически эффективной и согласованной системы контроля по защите информации во всех подразделениях Компании.

4.3.2. Определение и установление необходимого баланса между потребностью в свободном обмене и использовании информационных ресурсов Компании и допустимыми ограничениями на ее распространение;

4.3.3. Разработка и внедрение соответствующих регламентирующих документов и координация деятельности подразделений Компании в отношении обеспечения информационной безопасности;

4.3.4. Совершенствование информационной структуры, применение и развитие новых информационных технологий для поддержания устойчивого конкурентоспособного положения Компании на рынке.

5. Объекты информатизации как объекты защиты

5.1. Защищаемая информация

5.1.1. Под защищаемой информацией Компании понимается информация, создаваемая в процессе деятельности Компании, либо получаемая ей на основании закона или договорных отношений. Уничтожение, модифицирование, блокирование, нарушение конфиденциальности, доступности или целостности такой информации может нанести материальный ущерб Компании или ущерб её деловой репутации.

5.1.2. Информация, а также иные виды активов Компании являются её собственностью и представляются работнику только для выполнения своих должностных обязанностей. Компания оставляет за собой право осуществлять контроль надлежащего выполнения сотрудниками своих должностных обязанностей.

5.1.3. К защищаемой в Компании информации относится:

- информация, составляющая коммерческую тайну Компании;
- информация, обеспечение защиты которой возлагается на Компанию действующим законодательством (персональные данные, служебная тайна);
- свободно распространяемая информация о деятельности Компании, несанкционированное модифицирование и/или уничтожение которой может нанести материальный ущерб или ущерб деловой репутации Компании (например, информация, размещаемая на открытых и внутренних сайтах Компании и др.);

- информация в технологических системах управления производством производственных подразделений Компании;
- информационные ресурсы, содержащие сведения, охраняемые авторским правом;
- служебная информация, требующая защиты в соответствии с требованиями владельцев соответствующих информационных ресурсов.

5.1.4. Перечни защищаемой информации (информационных ресурсов, сведений) определяются Компанией в соответствующих внутренних нормативных документах (перечнях), утверждаемых руководством Компании.

5.1.5. Защищаемая информация может быть представлена на различных материальных носителях, к которым относятся:

- бумажные носители информации (документы);
- машинные носители информации (магнитные, магнитно-оптические, оптические, flash-накопители, карты памяти различных типов и др.);
- материальными носителями информации могут являться электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта защищаемая информация, передаваемая, хранимая или обрабатываемая при помощи технических средств (систем), а также обсуждаемая в помещениях при проведении мероприятий конфиденциального характера.

5.1.6. Защищаемая информация может быть, также, представлена в виде электронных сообщений (электронных документов), к которым относится информация, передаваемая или получаемая пользователями ИС Компании.

5.1.7. Перечисленные виды информации, независимо от особенностей её материальных носителей подлежат защите от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут привести к нанесению существенного ущерба Компании, её партнёрам и контрагентам, а также гражданам (субъектам информационных отношений).

5.2. Виды и характеристики информации

5.2.1 В Компании хранится и обрабатывается информация двух видов открытая и закрытая.

5.2.2 "Открытая" – на ее распространение и использование не имеется никаких ограничений; порядок предоставления регулируется соответствующими положениями и регламентами Компании;

5.2.3 "Закрытая" – информация, неизвестная другим лицам, доступ к которой должен быть ограничен с целью предупреждения или уменьшения риска завладения этой информацией злоумышленниками, конкурентами. Она разделяется на подвиды:

5.2.3.1 Конфиденциальная информация – не являющаяся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам и содержащиеся в перечне сведений конфиденциального характера, доступ к которой ограничивается в соответствии с законодательством РФ, а именно;

- коммерческая тайна;
- персональные данные;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
- сведения, составляющие тайну следствия и судопроизводства;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами

2018

(врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

5.2.3.2 Служебная информация:

– требующая защиты в соответствии с требованиями владельцев соответствующих информационных ресурсов;

– вся оставшаяся информация Компании по различным причинам не отнесенная к конфиденциальной и открытой.

5.2.4 Для хранения информационных ресурсов в ИС используются файловые серверы, а также базы данных. Они используются для централизованного хранения различной производственно-справочной информации (учет, логистика и т. п.).

5.3. Защищаемые ИС

5.3.1 Защищаемая информация не может быть рассмотрена в отрыве от систем обработки информации, на которых она циркулирует (хранится, обсуждается), поэтому точкой приложения усилий по защите являются ИС Компании, в том числе входящие в эти системы ресурсы (активы) Компании.

5.3.2 В ИС Компании могут входить:

– средства и объекты информатизации, к которым относятся объекты, узлы, элементы, составляющие техническую инфраструктуру корпоративной сети Компании (информационно-вычислительные комплексы, сети, системы связи и передачи данных, технические средства приема, передачи и обработки информации, а также другие технические средства;

– программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации;

– помещения, специально предназначенные для проведения мероприятий, связанных с обсуждением защищаемой информации (защищаемые помещения).

5.4. Субъекты отношений

5.4.1 Субъекты отношений непосредственно обращаются с ресурсами Компании или участвуют в процессе обеспечения их защиты. Субъекты имеют права и обязанности по отношению к объекту защиты и несут ответственность, установленную законодательством Российской Федерации.

5.4.2 Основными субъектами в контексте данной Политики являются:

– Компания, как обладатель создаваемых в процессе её деятельности информационных ресурсов ограниченного доступа или переданных ей на законном основании информационных ресурсов, принадлежащих третьим лицам;

– владельцы информационных ресурсов, систем;

– должностные лица и работники Компании, а также взаимодействующих организаций, учреждений, юридических лиц, как пользователи информационных ресурсов;

– контрагенты и партнёры Компании;

– органы исполнительной власти субъектов Российской Федерации;

– структурные подразделения Компании, а также внешние специализированные организации, обеспечивающие эксплуатацию технических средств обработки информации Компании и средств их обеспечения;

– другие юридические и физические лица, причастные к созданию и функционированию объектов информатизации Компании;

– иные лица, имеющие возможность обращаться с ресурсами Компании.

5.5. Организационная структура

5.5.1 Зоны ответственности по обслуживанию ИС разделены между подразделениями по территориальному принципу. Зоны ответственности по обеспечению требований информационной безопасности также распределяются по территориям, работы координируются в Дирекции по защите ресурсов и выполняются в территориальных отделах службы безопасности, филиалах и дочерних зависимых обществах.

5.5.2 Персонал структурных подразделений Компании и пользователи ИС Компании (независимо от их принадлежности) принимают участие в обеспечении информационной безопасности – в части исполнения предписанных правил безопасности информации.

5.5.3 Для рассмотрения вопросов обеспечения информационной безопасности по решению Генерального директора может создаваться управляющий комитет по ИБ. Роли в нем определяются приказом по Компании.

6. Основные факторы, влияющие на информационную безопасность

6.1. Основными факторами, влияющими на информационную безопасность Компании, являются:

- 6.1.1 автоматизация бизнес-процессов в Компании;
- 6.1.2 расширение кооперации исполнителей при построении и развитии информационной инфраструктуры Компании;
- 6.1.3 рост объемов информации Компании, передаваемой в ИС;
- 6.1.4 территориальная распределенность Компании;
- 6.1.5 рост компьютерных преступлений, в том числе из-за создания организованных преступных групп;
- 6.1.6 рост объемов информации, раскрываемой во внешней среде в соответствии с законодательством;
- 6.1.7 усиление роли регуляторов в области информационной безопасности;
- 6.1.8 увеличение количества угроз при международном взаимодействии.

7. Основные принципы обеспечения информационной безопасности

7.1. Построение архитектуры СУИБ Компании базируется на соблюдении следующих основных принципов обеспечения ИБ:

7.1.1 Простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов сетевого взаимодействия. Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного развития);

7.1.2 Апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку;

7.1.3 Построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью;

7.1.4 Управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей;

7.1.5 Простота эксплуатации, автоматизация максимального числа действий администраторов сети;

7.1.6 Эшелонированность обороны – для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание

защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невязаных областях;

7.1.7 Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств – системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода систем в незащищенное состояние;

7.1.8 Равнопрочность обороны по всем направлениям – осуществляется регламентация и документирование всех способов доступа к ресурсам ИС. В соответствии с этим принципом запрещается создавать несанкционированные подключения к ИС и другими способами нарушать установленный порядок предоставления доступа к информационным ресурсам, который определяется внутренними нормативными документами Компании;

7.1.9 Проактивная защита, основанная на профилактике нарушений безопасности. В большинстве случаев для Компании экономически оправданным является принятие предупредительных мер по недопущению нарушений безопасности в отличие от мер по реагированию на инциденты, связанных с принятием рисков осуществления угроз информационной безопасности. Однако это не исключает необходимости принятия мер по реагированию на инциденты и восстановлению поврежденных информационных ресурсов. В соответствии с данным принципом должен проводиться анализ рисков, опирающийся на модель угроз безопасности и модель нарушителя, определяемые настоящей Политикой. Многие риски можно уменьшить путем принятия превентивных мер защиты;

7.1.10 Минимизация привилегий - политика безопасности строится на основе принципа «все, что не разрешено, запрещено». Права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей;

7.1.11 Разделение обязанностей между администраторами ИС, определяется должностными инструкциями и регламентами администрирования.

7.1.12 Экономическая целесообразность. Обеспечение соответствия ценности информационных ресурсов Компании и величины возможного ущерба (от их разглашения, утраты, утечки, уничтожения и искажения) уровню затрат на обеспечение информационной безопасности. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы ИС Компании, в которых эта информация циркулирует.

7.1.13 Преемственность и непрерывность совершенствования. Обеспечение постоянного совершенствования мер и средств защиты информационных ресурсов и информационной инфраструктуры на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования систем защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого передового отечественного и зарубежного опыта в этой области.

8. Организация работ по защите информации

8.1. На основе настоящей Политики формируются подчиненные документы, которые описывают:

8.1.1 **Основные принципы формирования перечня критичных ресурсов**, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень включает в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для Компании;

8.1.2 **Основные принципы защиты**, определяющие стратегию обеспечения ИБ, и перечень правил, которыми необходимо руководствоваться при построении СУИБ Компании;

8.1.3 **Основные подходы к организации работ по защите информации** в Компании, распределение ролей и порядок взаимодействия подразделений Компании при осуществлении мероприятий по обеспечению информационной безопасности, разработке и согласовании организационно-распорядительных документов;

8.1.4 **Порядок категорирования защищаемой информации** и основные подходы к обеспечению безопасности различных категорий информационных ресурсов;

8.1.5 **Модель нарушителя безопасности**, определяемую на основе обследования ресурсов системы и способов их использования;

8.1.6 **Модель угроз безопасности и основные подходы к оценке рисков**, связанных с их осуществлением, формируемых на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;

8.1.7 **Требования безопасности** для каждой из основных подсистем информационной безопасности, определяемые по результатам оценки рисков;

8.1.8 **Меры обеспечения безопасности** организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований.

8.2. Для организации работ по защите информации в Компании определяется комплекс мероприятий, которые указаны в следующих пунктах и включают в себя планирование, выполнение, проверку и действие. Данные меры выполняются циклично, что позволяет производить постоянное улучшение состояния информационной безопасности.

8.3. Получение поддержки руководства Компании по реализации мер по защите информации:

8.3.1 Назначение ролей и распределение ответственности, которые закрепляются в положениях о подразделениях и должностных инструкциях;

8.3.2 Разработка, реализация, внедрение стандартов информационной безопасности и других документов по обеспечению ИБ;

8.3.3 Определение задач и планов мероприятий по реализации защиты;

8.3.4 Анонсирование по Компании важности следования требованиям документов по ИБ;

8.3.5 Обеспечение достаточных ресурсов для разработки, реализации и внедрения СУИБ;

8.3.6 Определение приемлемого уровня риска по Компании;

8.3.7 Подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ;

8.4. Выбор области применения мер по защите информации:

8.4.1 Выбор группы специалистов, которые помогут определить защищаемые бизнес-процессы;

8.4.2 Определить активы из которых состоят эти бизнес-процессы и какие из них подлежат защите;

8.4.3 Определить границы бизнес-процессов на которых происходит взаимодействие с другими организациями;

8.4.4 Определить требования со стороны контролирующих органов и стандартов в области ИБ.

8.5. Определение методики оценки рисков:

8.5.1 Выбор применимой методики оценки риска для определенных информационных активов;

8.5.2 Определение неприемлемых рисков, которые необходимо снижать;

8.5.3 Определение механизмов управления остаточными рисками.

8.6. Подготовка инвентаризации информационных активов для защиты и ранжирования в соответствии выбранной методикой оценки рисков:

8.6.1 Инвентаризация информационных активов;

8.6.2 Ранжирование уровней риска;

8.6.3 Определение риска, его классификация в соответствии с важностью и наличием уязвимостей;

8.6.4 Оценка значения риска и определение приемлемых и неприемлемых рисков в зависимости от уровня;

8.6.5 Принятие решения об управлении риском.

8.7. Управление рисками и план обработки рисков:

8.7.1 Принятие плана обработки рисков (принятие, передача, снижение, избегание);

8.7.2 Идентификация контролей и определение необходимых дополнительных контролей при помощи анализа недочетов;

8.7.3 Предложение по проектированию, развертыванию и совершенствованию организационной и технической инфраструктуры СУИБ;

8.8. Установление стандартов и других документов для контроля рисков:

8.8.1 Разработка стандартов и других документов с конкретными контрольными процедурами и назначением ответственных за них.

8.9. Выделение ресурсов и обучение персонала для реализации мероприятий по проектированию, развертыванию и совершенствованию инфраструктуры СУИБ.

8.10. Мониторинг применения СУИБ:

8.10.1 Периодические проверки и аудит ИБ Компании.

8.11. Периодический пересмотр требований ИБ Компании, включая непрерывное улучшение мер защиты, корректирующих и превентивных действий по защите информационных активов.

9. Ответственность сотрудников

9.1. Подготовка настоящего документа, внесение в него изменений и общий контроль выполнения требований ИБ сотрудниками Компании осуществляется подразделением ИБ.

9.2. Неукоснительное соблюдение правил, устанавливаемых настоящей Политикой обязательно для всех сотрудников Компании.

9.3. Руководители всех уровней несут прямую ответственность за выполнение положений настоящей Политики в подконтрольных им подразделениях.

9.4. Сотрудники Компании, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям в соответствии с трудовым законодательством РФ.

9.5. Сотрудники Компании должны быть ознакомлены с положениями настоящей Политики информационной безопасности и должны твердо их придерживаться.

9.6. Сотрудники Компании отвечают за:

9.6.1 понимание и соблюдение соответствующих Федеральных законов, политик, стандартов и процедур Компании в области информационной безопасности и связанных с ними последствий;

9.6.2 неиспользование или ненадлежащее использование доступных механизмов безопасности для защиты информации;

9.6.3 передачу и совместное использование служебных кодов, паролей и электронных средств доступа к информационным ресурсам, в помещения и к средствам обработки, передачи и защиты информации;

9.6.4 уведомления руководства по доступным каналам о нарушениях системы защиты или обнаруженных отказах;

9.6.5 осуществление намеренного изменения, уничтожения, чтения, или передачи информации неавторизованным способом, а также за создание препятствий в доступе к информации другим сотрудникам;

9.6.6 попытки подбора кодов доступа, паролей и других способов получения доступа к информационным системам, ресурсам и средствам обработки, передачи и защиты информации.

9.7. Владельцы информационных ресурсов несут ответственность за:

9.7.1 разработку стандартов и процедур, регулирующих её подготовку, сбор, обработку, распространение и удаление;

9.7.2 установление правил надлежащего использования и защиты информации в информационных системах, и сохраняет её, даже тогда, когда информация используется совместно с другими организациями;

9.7.3 предоставление сведений относительно требований информационной безопасности и контроля безопасности для систем, где информация обрабатывается, хранится и передаётся.

9.8. Владельцы информационных систем несут ответственность за:

9.8.1 закупку, развитие, интеграцию, модификацию, эксплуатацию, обслуживание и удаление информационной системы;

9.8.2 решение оперативных вопросов пользователей системы (например, пользователей, которым необходим доступ к информационной системы для выполнения бизнес, или оперативных задач) и соблюдение требований информационной безопасности;

9.8.3 развитие и поддержание плана по обеспечению безопасности (скоординированного с подразделением ИБ) и гарантируют, что система разворачивается и действует в соответствии с согласованным требованиями безопасности;

9.8.4 решение (скоординированное с владельцем информации) о предоставлении доступа к системе (об уровне установленных привилегий или прав доступа) и доведение необходимых требований безопасности при работе в системе до пользователей;

9.8.5 организацию вспомогательного обучения пользователей и обслуживающего персонала системы;

9.8.6 информирование соответствующих должностных лиц о необходимости проведения авторизации, обеспечение наличия ресурсов, необходимых для деятельности, и предоставление доступа к системе, информации и документации по безопасности.

9.9. Сотрудники, имеющие расширенные привилегии доступа к информационным ресурсам и активам, выполняющие служебные обязанности по администрированию средств, обеспечивающих функционирование информационных систем и средств обеспечения информационной безопасности, отвечают за:

9.9.1 корректное применение доступных механизмов и средств защиты для осуществления положений Политики;

9.9.2 уведомление руководства о неработоспособности существующих средств защиты и любых технических соображениях, которые могли бы улучшить их эффективность;

9.9.3 оперативное и эффективное восстановление работоспособности информационных систем и устранение последствий нарушений информационной безопасности;

9.9.4 уведомление владельцев информационных ресурсов о выявленных фактах успешных и неуспешных попыток несанкционированного доступа к защищенным ресурсам;

9.9.5 использование доступных средств аудита для облегчения обнаружения нарушений безопасности;

2018

9.9.6 наличие и ведение журналов о фактах доступа сотрудников к защищаемым информационным ресурсам и связанным с ними техническими средствами и помещениями;

9.9.7 отслеживание информации о вновь разрабатываемых методах и средствах обеспечения информационной безопасности и уведомление руководства Компании и владельцев информационных ресурсов о соответствующих изменениях или новых разработках.

9.10. Отношения между работником и работодателем и соответствующая ответственность за нарушение ИБ организации регулируются Трудовым кодексом РФ.

10. Механизм реализации Политики

10.1. Реализация Политики обеспечения информационной безопасности Компании осуществляется на основе утвержденных конкретных программ и планов, которые ежегодно уточняются с учетом:

- федерального законодательства в области защиты информации;
- международных и отраслевых стандартов в области информационной безопасности и ИТ безопасности;
- организационно - распорядительных документов Компании;
- реальных потребностей в средствах обеспечения информационной безопасности;
- объемов финансирования, выделяемых на обеспечение информационной безопасности Компании.

Лист регистрации изменений

[illegible]

¹ Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.