|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА - Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
|  |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №1** | |
| **по дисциплине** | |
| **«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»** | |
|  | |
| Выполнил студент группы БИСО-01-19 | **Зиатдинова Камилла Рафаилевна** |

Москва 2020

Организация JinHit Entertainment.

Штат — 84 сотрудников. 7- руководство, 12- бухгалтерия, 8 — IT-отдел, 34— менеджеры по работе с клиентами, 5 — отдел безопасности, 14 – юридический отдел, 4- отдел кадров.

Руководство Организации использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует телефонную связь, MS Office, 1С: Бухгалтерию.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др.

Отдел безопасности обеспечивает организацию системы безопасности и распределение ответственности между сотрудниками.

Юридический отдел использует телефонную связь, MS Office.

Отдел кадров использует телефонную связь, MS Office, 1C:Кадры.

**ВВОДНЫЕ ПОЛОЖЕНИЯ**

Настоящая Политика является основополагающим документом, предназначенным для выражения позиции Организации в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности бизнес-процессов Организации, создания условий безопасного цифрового развития Организации и обеспечения соответствия требованиям законодательства Российской Федерации в данной области, а также применимого законодательства любого иного государства, где Организация осуществляет деятельность.

Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

**ОБЛАСТЬ ДЕЙСТВИЯ**

Настоящая Политика обязательна для исполнения работниками JinHit Entertainment и подконтрольных Обществ Группы, в отношении которых уставами Обществ, акционерными и иными соглашениями с компаниями-партнерами не определен особый порядок реализации акционерами/участниками своих прав, в том числе по управлению Обществом.

**ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ**

Настоящая Политика является локальным нормативным документом постоянного действия. Настоящая Политика утверждается, изменяется и признается утратившей силу в JinHit Entertainment решением Совета директоров JinHit Entertainment и вводится в действие в JinHit Entertainment приказом JinHit Entertainment.

**ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящая Политика выражает позицию Организации в области информационной безопасности. Принятием настоящей Политики Организация провозглашает и обязуется осуществлять все возможные меры для защиты работников, имущества, информации, деловой репутации и бизнес-процессов Организации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Организации осознает важность и необходимость продвижения и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства РФ и регулирования норм информационной безопасности, а также развития используемых информационных технологий при автоматизации и цифровизации бизнес-процессов и технологических процессов на производствах. Соблюдение принципов информационной безопасности дополнительно позволит упрочить конкурентные преимущества Организации, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить имиджевые риски.

Настоящая Политика разработана с целью установления принципов, определяющих общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Организации и защиты интересов Организации от рисков и угроз информационной безопасности.

Руководство Организации придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является, в том числе, элементом корпоративной культуры. Следование требованиям информационной безопасности является важным условием при осуществлении повседневной деятельности (в том числе при реализации ИТ-проектов, проработке цифровых инициатив и т.д.), включая совместную работу с Деловыми партнерами. Каждый работник Организации и её Деловых партнеров несёт ответственность за безопасную работу с вверенными ему корпоративными ИТ-активами, компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Организации.

Руководители и специалисты по информационной безопасности Организации должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищённости информации, ИТ-активов, бизнес и технологических процессов Организации.

**СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ**

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ (АСУ) Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

КОМПЬЮТЕРНАЯ АТАКА Действия, направленные на реализацию угроз несанкционированного доступа к ИТ-активу, воздействия на него или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Организации.

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (ИТ-ИНФРАСТРУКТУРА) Совокупность компонентов информационных технологий, в том числе аппаратное (системы обработки и хранения данных, оборудование рабочего места, периферия и т.д.), системное программное и инженерное обеспечение, сети, специализированные помещения.

ИНФОРМАЦИОННАЯ СИСТЕМА (ИС) Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

ИНФОРМАЦИОННАЯ СРЕДА Совокупность разной информации вместе с ИТинфраструктурой, а также субъектами, которые занимаются сбором, использованием и распространением информации.

ИНФОРМАЦИОННОТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

ИНФОРМАЦИЯ Сведения (сообщения, данные) независимо от формы их представления.

ИТ-АКТИВ Идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Организации.

ИТ-ПРОСТРАНСТВО Совокупность объектов (информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура), вступающих друг с другом в информационное взаимодействие, а также сами информационные технологии, обеспечивающие данное взаимодействие.

ОРГАНИЗАЦИЯ Группа юридических лиц различных организационно-правовых форм, включая JinHit Entertainment, в отношении которых последнее выступает в качестве основного или преобладающего (участвующего) общества.

МОБИЛЬНОЕ ТЕХНИЧЕСКОЕ СРЕДСТВО Съемные машинные носители информации, портативные вычислительные устройства и устройства связи с возможностью обработки информации (переносные персональные компьютеры - ноутбуки, нетбуки, планшетные компьютеры, а также мобильные телефоны, смартфоны, умные часы/браслеты, цифровые камеры, звукозаписывающие устройства и иные средства).

ОБЩЕСТВО ГРУППЫ (ОГ) Хозяйственное общество, прямая и (или) косвенная доля владения JinHit Entertainment акциями или долями в уставном капитале которого составляет 20 процентов и более.

ПОДКОНТРОЛЬНОЕ ОБЩЕСТВО ГРУППЫ Общество Группы, в котором JinHit Entertainment имеет право прямо и/или косвенно (через подконтрольных ему лиц) распоряжаться в силу участия в таком Обществе Группы и (или) на основании договоров доверительного управления имуществом, и (или) простого товарищества, и (или) поручения, и (или) акционерного соглашения, и (или) иного соглашения, предметом которого является осуществление прав, удостоверенных акциями (долями) такого Общества Группы, более 50 процентами голосов в высшем органе управления, либо назначать (избирать) единоличный исполнительный орган и/или более 50 процентов состава коллегиального органа управления.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

ПРОИЗВОДСТВЕННАЯ СИСТЕМА Совокупность компонентов информационных технологий, обеспечивающих автоматизацию решения задач планирования и управления различными видами производственной деятельности и производственных процессов.

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБРИСК) Сочетание вероятности реализации угрозы информационной безопасности и последствий её реализации, оказывающих негативное влияние на достижение целей Организации.

СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ Структурное подразделение JinHit Entertainment или Общества Группы с самостоятельными функциями, задачами и ответственностью в рамках своих компетенций, определенных в Положении о структурном подразделении.

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (УГРОЗА) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива.

УЯЗВИМОСТЬ ИТ-АКТИВА Недостаток (слабость) ИТ-актива в целом, который(ая) может быть использован(а) для реализации угроз информационной безопасности.

ЦИФРОВИЗАЦИЯ Применение прорывных технологий, трансформирующих операционные процессы за счет замещения или дополнения человека на базе использования качественно новой аналитики, искусственного интеллекта, мобильных и носимых устройств, роботизации, интеграционных технологических платформ.

ДЕЛОВОЙ ПАРТНЕР Текущие и потенциальные контрагенты JinHit Entertainment, а также Обществ Группы.

РУКОВОДИТЕЛИ И СПЕЦИАЛИСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ Руководители и/или работники структурного подразделения JinHit Entertainment/Общества Группы, ответственного за координацию, планирование и организацию функционирования процессов в области информационной безопасности и за операционное управление ими.

ТРЕТЬИ ЛИЦА Хозяйственные общества, в которых JinHit Entertainment не имеет прямой либо косвенной доли в уставных капиталах, некоммерческие организации, в состав органов управления которых не входят представители Организации, а также лица, не являющиеся работниками и не занимающие должности в органах управления JinHit Entertainment и Обществ Группы.

РОЛИ ДЛЯ ЦЕЛЕЙ НАСТОЯЩЕГО ДОКУМЕНТА РУКОВОДСТВО ОРГАНИЗАЦИИ Главный исполнительный директор JinHit Entertainment, топ-менеджеры JinHit Entertainment, единоличные исполнительные органы Обществ Группы.

**ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ**

Основными объектами защиты системы информационной безопасности в Организации являются:

* информационные ресурсы, содержащие государственную и коммерческую тайны, сведения ограниченного распространения, конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Организации, независимо от формы и вида ее представления;
* сотрудники Организации, являющиеся разработчиками и пользователями информационных систем Организации;
* информационная инфраструктура, включающая системы хранения, обработки и анализа информации, программные и программно-аппаратные средства ее 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.

**ЦЕЛИ И ЗАДАЧИ ОРГАНИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Управление и обеспечение информационной безопасности Организации ориентированы на достижение следующих целей в области информационной безопасности:

* предоставление безопасной информационной среды для функционирования и развития бизнес-процессов Организации;
* снижение уровня ИБ-рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое цифровое развитие Организации.

Для достижения данных целей необходимо решение следующих задач:

* обеспечение информационной безопасности бизнес-процессов Организации в условиях возрастающего уровня угроз, включая обеспечение оперативного мониторинга и оценку состояния защищенности в Организации; повышение эффективности защиты от спланированных целенаправленных компьютерных атак злоумышленниками; повышение информационной безопасности технологических и производственных систем;
* применение новых современных методов для защищенной цифровизации Организации, включая организацию проработки вопросов информационной безопасности при реализации цифровых решений; организацию апробации и применения новых методов защиты информации от современных угроз, в том числе за счет взаимодействия и партнерства с лидерами отрасли информационной безопасности; обеспечение применения безопасных цифровых технологий при внедрении отечественных разработок и развитии собственного конкурентоспособного корпоративного программного обеспечения Организации;
* соответствие требованиям государства в области информационной безопасности путем обеспечения заданного уровня информационной безопасности ИТ-активов в соответствии с требованиями действующего законодательства стран присутствия Организации.

**УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Организации и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре Организации могут быть как внешними, так и внутренними.

**МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

По отношению к Организации нарушители могут быть разделены на внешних и внутренних нарушителей.

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Организацией рассматриваются:

* зарегистрированные пользователи информационных систем Организации;
* сотрудники Организации, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Организации, но имеющие доступ в здания и помещения;
* персонал, обслуживающий технические средства корпоративной информационной системы Организации;
* сотрудники подразделений Организации, задействованные в разработке и сопровождении программного обеспечения;
* сотрудники подразделений, обеспечивающие безопасность Организации;
* руководители различных уровней

Внешние нарушители.

В качестве потенциальных внешних нарушителей Организацией рассматриваются:

* бывшие сотрудники Организации;
* представители организаций, взаимодействующих по вопросам программного и программно-аппаратного обеспечения Организации;
* посетители зданий и помещений Организации;
* конкурирующие с Организацией прочие организации;
* члены преступных организаций, сотрудники спецслужб или действующие по их заданию;
* лица, случайно или умышленно проникшие в корпоративную информационную систему Организации из внешних телекоммуникационных сетей (хакеры).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

* нарушитель скрывает свои несанкционированные действия от других сотрудников Организации;
* несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения информации;
* в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей:
* внешний нарушитель может действовать в сговоре с внутренним нарушителем

**ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Деятельность Организации в области информационной безопасности осуществляется с соблюдением следующих основных принципов.

Ориентация на стратегию Организации – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития Организации, с учетом корпоративных стратегий в области информационных технологий и в области производственной автоматизации, метрологии и контроля качества.

Централизация функций управления – принцип заключается в возможности принятия управленческих решений в области информационной безопасности на уровне Организации за счет оперативного мониторинга (ИТ-пространства Организации и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности; осуществления централизованного управления стратегическими инициативами по информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности; создания и развития централизованных решений в области информационной безопасности.

Проактивный подход и управление рисками – базируется на мониторинге, анализе и оценке появляющихся, актуальных и будущих ИБ-рисков и угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Организации.

Стандартизация и унификация – подразумевает разработку и тиражирование в ОГ стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения информационной безопасности для унификации средств и методов решения однотипных задач; интерфейсов управления системами информационной безопасности.

Импортозамещение – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счёт ориентирования на отечественные решения, средства и сервисы при обеспечении информационной безопасности на территории Российской Федерации.

Ресурсное обеспечение – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной безопасности Организации, поддержание требуемой организационной структуры.

Законность и соответствие – деятельность по обеспечению информационной безопасности Организации основывается на выполнении требований нормативных правовых актов Российской Федерации и национального законодательства стран, на территории которых осуществляют деятельность зарубежные ОГ.

Повышение культуры информационной безопасности – декларирует необходимость не только информировать всех работников Организации, её Деловых партнёров и третьих лиц использующих ИТ-активы Организации, о требованиях информационной безопасности, но развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами Организации.

Развитие компетенций и профессионализма – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей. Обеспечение информационной безопасности при автоматизации технологических и производственных процессов требует компетенций и знаний в областях производственной автоматизации и метрологии.

Накопление знаний и обмен опытом – следует накапливать знания и обмениваться опытом в ходе осуществления практической деятельности по обеспечению информационной безопасности (при мониторинге и реагировании на компьютерные атаки, при внедрении и эксплуатации технических решений, при аудитах информационной безопасности и т.д.).

Информационная безопасность как неотъемлемое свойство ИТ-актива – принцип заключается в следующем:

* требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива, вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе;
* создание программных продуктов в интересах Организации осуществляется с применением методов безопасной разработки программного обеспечения;
* предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);
* встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;
* соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

Информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги) – означает, что предлагаемые и оказываемые Организации или в интересах Организации ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

Совместимость – подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость на информационном, программном, электромагнитном и эксплуатационном уровнях, а также совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации технологических и производственных процессов Организации.

Надежность – использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

Адекватность и обоснованность решений – принимаемые в Организации меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Организации.

Комплексность – применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба Организации, её Деловым партнёрам и работникам.

Разделение и минимизация полномочий – означает, что выполнение критичных (итоговых) операций проводится только посредством разделения действий (например, алгоритмического разделения, временного или ресурсного - в т.ч. двумя работниками). Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделений полномочий является предпочтительным относительно организационного. Должны осуществляться контроль реализации принципов разграничения критических полномочий в ИС и в АСУ, ограничение прав доступа, в зависимости от уровня согласованных полномочий. Полномочия должны быть минимально достаточными для выполнения лицом своих должностных обязанностей, либо выполнения контрактных обязательств. При необходимости должен осуществляться контроль конфликта полномочий – организационный, а также программно-аппаратный.

Постоянство совершенствования информационной безопасности – обеспечение постоянного улучшения существующей практики и совершенствования средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области.

**ОСНОВНЫЕ ЦЕЛИ ПОЛИТИКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:**

* обеспечение адекватной защиты информационных ресурсов Организации с использованием организационно-технических мер обеспечения информационной безопасности;
* создание комплексной и эффективной системы обеспечения и управления информационной безопасности Организации, соответствующей отраслевым требованиям и стандартам
* обеспечение соответствия требованиям законодательства Российской Федерации в области защиты информации.

**ОСНОВНЫЕ МЕТОДЫ ДОСТИЖЕНИЯ ЦЕЛЕЙ ПОЛИТИКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:**

* обеспечение выполнения требований отраслевых документов в области информационной безопасности;
* определение функциональных обязанностей и ответственных работников и подразделений Организации в области информационной безопасности;
* обеспечение поддержки и управления в области информационной безопасности со стороны руководства Организации;
* определение структуры и принципов организации процессов управления информационной безопасностью, систем организационно-распорядительной и методологической документации в области информационной безопасности;
* обеспечение соответствия нормативно-методической организационно-распорядительной документации по обеспечению информационной безопасности Организации отраслевым требованиям и стандартам;
* определение и внедрение комплекса организационных и технических мер, направленных на обеспечение выполнения требований в области информационной безопасности;
* определение процедур независимого контроля выполнения требований в области информационной безопасности Организации.

**ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ ИБ**

Общее руководство обеспечением информационной безопасности осуществляет начальник ОСБ.

Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности является начальник ОСБ.

Нарушение требований Политики, локальных нормативных актов по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между руководством и сотрудниками.

Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется в каждом конкретном случае

Руководители структурных подразделений, несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в ОСБ о всех инцидентах, связанных с нарушениями требований информационной безопасности.

Руководители структурных подразделений обязаны незамедлительно сообщать в ОСБ о всех происшествиях и нештатных ситуациях в сфере их деятельности связанных с информационной безопасностью.

Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Организации, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

Ответственность сотрудников Организации за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с сотрудниками Организации, а также положениями внутренних нормативных документов Организации

Виды ответственности, предусмотренные федеральными законами об обращении с информацией конфиденциального характера:

* гражданско-правовая ответственность
* дисциплинарная ответственность
* уголовная ответственность
* административная ответственность

**ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

Требования настоящей Политики могут развиваться другими внутренними нормативными документами Организации, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также Устава Организации настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Организации. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

Пересмотр и в случае необходимости внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

* пересмотр настоящей Политики должен осуществляться не реже одного раза в 12 месяцев;
* внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Ответственным за внесение изменений в настоящую Политику является руководитель Ответственного подразделения.