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

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 1** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Маринин Вячеслав Петрович |
|  |

Москва 2020

Оглавление

[1. **Общие положения** 3](#_Toc54029198)

[2. **Список терминов и определений** 4](#_Toc54029199)

3. **Область действия**...............................................................................................................................6

[4. **Система защиты персональных данных** 7](#_Toc54029200)

[5. **Цели и задачи деятельности по обеспечению информационной безопасности** 8](#_Toc54029201)

[6. **Угрозы информационной безопасности** 9](#_Toc54029202)

7.  [**Модель нарушителя информационной безопасности** 11](#_Toc54029203)

[8. **Общие требования по обеспечению ИБ** 11](#_Toc54029205)

[9](#_Toc54029206)**. Ответственность в сфере ИБ 11**

**1. Общие положения**

Политика информационной безопасности ООО «Небо» определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми в последствии руководствуется в своей деятельности.

Мероприятия по обеспечению информационной безопасности являются составной частью управленческой, производственной деятельности Компании и должны осуществляться на постоянной основе во взаимосвязи с другими мерами по обеспечению установленного режима функционирования ИС Компании.

Совокупность защитных мероприятий, реализующих обеспечение ИБ и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет СИБ.

Совокупность защитных мер и процессов их эксплуатации должна обеспечивать ИБ на требуемом уровне, а именно - обеспечивать ИБ в условиях штатного функционирования ИС, а также в условиях реализации актуальных угроз, учтенных при анализе рисков.

Для поддержания ИБ на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Управление событиями и инцидентами безопасности, полученными в результате мониторинга, позволяет избежать деградации и обеспечить требуемый уровень ИБ объектов защиты.

В процессе деятельности Компании должны учитываться риски нарушения ИБ, которые выражаются в возможности нарушения ИБ объектов защиты и возникновения ущерба Компании. Анализ и оценка рисков нарушения ИБ.

Правовой основой Политики являются:

* Конституция Российской Федерации;
* Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»;
* Закон Российской Федерации № 5485-1 от 21.07.1993 «О государственной тайне»;
* Доктрина информационной безопасности Российской Федерации (5 декабря 2016 г. №646);
* Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон № 99-ФЗ от 04.05.2011 «О лицензировании отдельных видов деятельности»;

Кодекс Российской Федерации об административных правонарушениях (от 30.12.2001 N 195-Ф3);

* Внутренние нормативно – методические и организационно – распорядительные документы;
* Федеральный закон № 126-ФЗ от 07.07.2003 «О связи»;
* Кодекс Российской Федерации об административных правонарушениях (от 30.12.2001 N 195-Ф3);
* Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;

Основные положения Политики распространяются на все структуры и подразделения Общества. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений (в том числе дочерние), осуществляющие взаимодействующие с АС в качестве поставщиков и потребителей (пользователей) информации АС.

**2. Список терминов и определений**

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Внешняя информационная система** – информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

**Вредоносная программа** – программа, предназначенная для осуществ­ления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

**Государственные информационные системы** – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

**Доступ в операционную среду компьютера** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступность информации** – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

**Закладочное устройство** – элемент средства съёма информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съёма информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, обрабатываемая в информационной системе.

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

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информация ограниченного доступа** – информация, доступ к которой ограничен федеральными законами.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона**– пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

**Конфиденциальность информации** – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информацион­ной системы.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, коли­чественных характеристик физических величин.

**Общедоступная информация** – это общеизвестные сведения и иная информация, доступ к которой не ограничен.

**Оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

**Техническое средство** – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

**Перехват (информации)** – неправомерное получение информации с ис­пользованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь** – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесённый в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

**3. Область действия**

Требования настоящей Политики распространяются на всех сотрудников Учреждения, а также всех прочих лиц (подрядчики, аудиторы и т.п.).

**4. Система защиты персональных данных**

Система защиты персональных данных (СЗПДн), строится на  основании:

- отчета о результатах проведения внутренней проверки;

- перечня персональных данных, подлежащих защите;

- акта классификации информационной системы персональных данных;

- модели угроз безопасности персональных данных;

- положения о разграничении прав доступа к обрабатываемым ПДн.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверки, сделаны выводы о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн готовится список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты включает:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечение целостности данных;

- обнаружение вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

# 5. Цели и задачи деятельности по обеспечению

# информационной безопасности

Цели защиты информации:

-предотвращение угроз безопасности предприятия вследствие несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации или иных форм незаконного вмешательства в информационные ресурсы и информационных системах;

-сохранение коммерческой тайны, обрабатываемой с использованием средств вычислительной техники;

-защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

Для достижения целей защиты должно обеспечиваться эффективное решение следующих задач:

· защита от вмешательства в процесс функционирования предприятия посторонних лиц;

· защита от несанкционированных действий с информационными ресурсами предприятия посторонних лиц и сотрудников, не имеющих соответствующих полномочий;

· обеспечение полноты, достоверности и оперативности информационной поддержки принятия управленческих решений руководством предприятия;

· обеспечение физической сохранности технических средств и программного обеспечения предприятия и защита их от действия техногенных и стихийных источников угроз;

· регистрация событий, влияющих на безопасность информации, обеспечения полной подконтрольности и подотчетности выполнения всех операций, совершаемых на предприятии;

· своевременное выявление, оценка и прогнозирование источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба интересам субъектов, нарушению нормального функционирования и развития предприятия;

· анализ рисков реализации угроз безопасности информации и оценка возможного ущерба, предотвращение неприемлемых последствий нарушения безопасности информации предприятия, создание условий для минимизации и локализации наносимого ущерба;

· обеспечение возможности восстановления актуального состояния предприятия при нарушении безопасности информации и ликвидации последствий этих нарушений;

· создание и формирование целенаправленной политики безопасности информации предприятия.

# 6. Модель нарушителя информационной безопасности

# Основными источниками защищаемой информации на объектах информатизации (ОИ) являются субъекты информационных отношений:

* пользователи (операторы), программисты, администраторы АС (ЛВС), руководители разработки и эксплуатации АС, технический (обслуживающий) персонал;
* документы на твердой основе, различного характера и назначения включая электронные документы на машиночитаемых носителях информации, с защищаемой информацией;
* штатные технические средства АС обработки защищаемой информации: АРМ, ЛВС, средства обеспечения производственной деятельности людей, информационные и телекоммуникационные линии связи.

*Под угрозами информационной безопасности* понимается потенциальная возможность нарушения её следующих основных, качественных характеристик (свойств):

* конфиденциальности (разглашение, утечка) сведений, составляющих государственную, служебную или коммерческую тайну, а также персональных данных;
* работоспособности (дезорганизация работы) программно-технических комплексов, блокирование информации, нарушение технологических процессов обработки информации, срыв своевременного решения выполняемых задач;
* целостности и достоверности информационных, программных и других ресурсов, а также фальсификация (подделка) документов.

Источники угроз информационной безопасности, разделяются на *внешние и внутренние*:

К внешним источникам угроз относятся:

* деятельность иностранных разведывательных и специальных служб, направленная на добывание защищаемых информационных ресурсов с ограниченным доступом, о подготавливаемых решениях и инициативах, в том числе по экономическим вопросам, а также на подрыв авторитета Организации;
* действия преступных групп, формирований и связанных с ними коррумпированных лиц по добыванию защищаемой информации в целях реализации своих преступных замыслов;
* использование средств опасного воздействия на информационные ресурсы, получение несанкционированного доступа к ним;
* недружественная политика иностранных государств в области распространения информации и новых информационных технологий;
* преступная деятельность отдельных лиц, бандитских групп и формирований или злоумышленников, конкурирующих и недобросовестных организаций, в том числе с использованием телекоммуникационных систем (прежде всего Интернет);
* промышленный шпионаж со стороны иностранных представителей при проведении совместных международных проектов и работ;
* диверсионные действия по отношению к объектам информатизации (поджоги, технические аварии, взрывы и т.д.);
* деятельность министерств и ведомств и субъектов Российской Федерации, препятствующая или умышленно создающая трудности работе системы, совершаемая в противовес принятых законодательных актов;
* стихийные бедствия, аварии, и техногенные катастрофы.

К внутренним источникам угроз относятся:

* неправомерные действия должностных лиц в области формирования, распространения и использования защищаемой информации;
* преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия персонала, работающего на объектах информатизации;
* отказы технических средств и программного обеспечения в информационных и телекоммуникационных системах;
* некомпетентные действия и ошибки, допущенные при проектировании и эксплуатации информационных систем;
* халатность и недостаточно четкое исполнение служебных обязанностей при проведении мероприятий по защите информации;
* нарушения пользователями (исполнителями работ) и обслуживающим персоналом установленных регламентов сбора, обработки и передачи информации, а также требований по защите информации;
* отказы, неисправности и сбои средств защиты информации и средств контроля эффективности, принятых мер по защите информации;
* непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия персонала при эксплуатации объектов информатизации, приводящие к разглашению защищаемой информации;
* нахождение в разных местах или отсутствие необходимых сил и финансовых средств, для реализации мер в организации и защите информационных ресурсов;
* противозаконная деятельность коммерческих и экономических структур, имеющих позиции в среде сотрудников и пользователей;
* получение криминальными структурами доступа к защищаемой информации, снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере.

**7. Модель нарушителя информационной безопасности**

Под **возможным нарушителем** (злоумышленником) для объектов информатизации подразумевается лицо или группа лиц, не состоящих или состоящих в сговоре, которые в результате преднамеренных или непреднамеренных действий потенциально могут нанести ущерб защищаемым ресурсам (информации).

Для принятия мер по обеспечению информационной безопасности защищаемой информации на объектах информатизации (обрабатывающих информацию с ограниченным доступом) в разрабатывается **модель возможного нарушителя** (применительно к конкретному ОИ), которая включает две категории возможных нарушителей — внешние и внутренние возможные нарушители.

Предполагается, что несанкционированный доступ на объекты информатизации посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

К внешним возможным нарушителям относится деятельность по добыванию конфиденциальной информации. При этом внешний возможный нарушитель ведет перехват, анализ и модификацию информации, передаваемой по каналам связи ОИ, проходящим вне контролируемой территории.

**8. Общие требования по обеспечению информационной**

**безопасности**

8.1 Назначение и распределение ролей и обеспечение доверия к персоналу

8.2 Управление жизненным циклом автоматизированных банковских систем

8.3 Управление доступом к информационным активам и регистрация событий

8.4 Антивирусная защита

8.5 Использование ресурсов Интернет

8.6 Использование средств криптографической защиты информации

8.7 Защита банковских платежных и информационных технологических процессов

8.8 Обеспечение защиты персональных данных

8.9 Обеспечение непрерывности бизнеса и восстановления после сбоев  
8.10 Обеспечение физической безопасности

**9. Ответственность в сфере ИБ**

9 .1.На начальника юридического отдела возлагается ответственность за контроль организации обработки защищаемой информации в соответствии с требованиями настоящей Политики.

9.2.На начальника ОЗИ возлагается ответственность за:

-организацию обработки защищаемой информации (как с применением средств автоматизации, так и без них) в соответствии с требованиями настоящей Политики, в том числе разработка документов на основе Политики, планирование мероприятий, согласование документов, влияющих на информационную безопасность;

- контроль исполнения требований Политики в структурных подразделениях Общества.

9.3.На руководителей структурных подразделений Общества возлагаются обязанности по обеспечению соблюдения установленного порядка обращения с защищаемой информацией в подчиненных им структурных подразделениях.

9.4.На начальника отдела информационных технологий возлагается ответственность за контроль соблюдения требований Политики и иных организационно-распорядительных документов Общества сотрудниками Общества при автоматизированной обработке защищаемой информации на рабочих местах.

9.5. Каждый работник Общества, имеющий доступ к защищаемой информации, несет ответственность за её искажение, разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности.

9.6. Работники Общества, разгласившие защищаемую в Обществе конфиденциальную информацию или нарушившие установленный порядок обращения с защищаемой информацией, а также работники, по вине которых произошла утрата конфиденциальных документов, нарушение работы информационных систем, ухудшающее доступность, целостность, конфиденциальность защищаемой информации, несут ответственность, предусмотренную законодательством Российской Федерации, внутренними документами Общества.