

УТВЕРЖДЕНО

приказом № 33 от «09» 06 2024

Директор ГАПОУ СО «ТМК»

И.А.Мочалов



П 361-2024

КОНЦЕПЦИЯ

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО
АВТОНОМНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»**

Тольятти, 2024 г.

ОГЛАВЛЕНИЕ

1. АННОТАЦИЯ	5
2. ОБЩИЕ ПОЛОЖЕНИЯ	6
2.1. Назначение и правовая основа документа	6
2.2. Объекты защиты.....	7
2.3. Категории информационных ресурсов, подлежащих защите	8
2.4. Цели обеспечения безопасности информации.....	9
2.5. Задачи обеспечения безопасности информации.....	10
2.6. Основные пути решения задач защиты информации.....	11
2.7. Угрозы безопасности информации и их источники.....	12
2.8. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации	14
2.9. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации.....	15
2.10. Пути реализации основных естественных угроз безопасности информации.....	16
2.11. Неформальная модель возможных нарушителей.....	17
3. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	21
3.1. Законность.....	21
3.2. Системность.....	22
3.3. Комплексность.....	22
3.4. Непрерывность защиты	22
3.5. Своевременность.....	23
3.6. Преемственность и совершенствование	23
3.7. Разумная достаточность (экономическая целесообразность)	23

3.8.	Персональная ответственность.....	24
3.9.	Минимизация полномочий.....	24
3.10.	Взаимодействие и сотрудничество	24
3.11.	Гибкость системы защиты	25
3.12.	Открытость алгоритмов и механизмов защиты.....	25
3.13.	Простота применения средств защиты.....	26
3.14.	Обоснованность и техническая реализуемость	26
3.15.	Специализация и профессионализм.....	26
3.16.	Обязательность контроля.....	26
4.	МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	28
4.1.	Законодательные (правовые) меры защиты	28
4.2.	Морально-этические меры защиты	28
4.3.	Технологические меры защиты	29
4.4.	Организационные (административные) меры защиты	29
4.4.1.	Формирование политики информационной безопасности	29
4.4.2.	Регламентация доступа в помещения.....	29
4.4.3.	Регламентация допуска сотрудников к использованию информационных ресурсов.....	30
4.4.4.	Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов.....	31
4.4.5.	Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов	32
4.4.6.	Подбор и подготовка персонала, обучение пользователей.....	32
4.4.7.	Ответственность за нарушения установленного порядка пользования ресурсами информационной системы Учреждения. Расследование/исследование нарушений.....	33

5. СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	34
5.1. Физические средства защиты	34
5.2. Программные и программно-аппаратные средства защиты информации	34
5.3. Средства управления системой информационной безопасности	35
5.4. Средства контроля эффективности системы защиты.....	36
6. ТЕХНИЧЕСКАЯ ПОЛИТИКА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	37
7. ФОРМИРОВАНИЕ РЕЖИМА БЕЗОПАСНОСТИ ИНФОРМАЦИИ.....	38
8. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ.....	41
9. ИСТОРИЯ ИЗМЕНЕНИЙ.....	42

1. АННОТАЦИЯ

Настоящий документ представляет собой концепцию обеспечения информационной безопасности в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее - Учреждение) и определяет:

- основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для Учреждения;

- основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (далее - ИБ) и перечень политик правил, которыми необходимо руководствоваться при построении системы защиты информации Учреждения;

- модель нарушителя безопасности, определяемую на основе обследования ресурсов Учреждения и способов их использования;

- модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;

- требования к информационной безопасности, определяемые по результатам анализа рисков;

- меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации требований безопасности;

- ответственность сотрудников Учреждения за соблюдение установленных требований ИБ при эксплуатации информационных систем (далее - ИС) Учреждения.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Назначение и правовая основа документа.

Концепция информационной безопасности (далее - Концепция) Учреждения определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, а также требований и базовых подходов к их реализации. В Концепции описывается общая стратегия обеспечения информационной безопасности Учреждения.

Методологической основой Концепции являются Российские и международные стандарты в области информационной безопасности.

Законодательной основой Концепции являются: Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

Концепция учитывает современное состояние и ближайшие перспективы развития информационных технологий в Учреждения, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений.

Основные положения Концепции базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

Концепция является методологической основой для:

1. формирования Политики информационной безопасности в Учреждения;
2. выработки комплекса согласованных мер по выявлению, отражению и нейтрализации угроз безопасности информации;
3. координации деятельности структурных подразделений Учреждения и ответственных лиц при проведении работ по созданию, развитию и эксплуатации информационных технологий;
4. разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения Политики информационной безопасности Учреждения.

Положения и требования Концепции распространяются на все структурные подразделения, входящие в состав Учреждения.

2.2. Объекты защиты

2.2.1. Основными объектами системы информационной безопасности Учреждения являются:

1. Информационные ресурсы, содержащие сведения, содержащие персональные данные, или иные критичные информационные ресурсы Учреждения;

2. Процессы обработки, хранения и передачи информации в информационных системах Учреждения, а также ее участники (пользователи и обслуживающий персонал);

3. Инфраструктура информационных систем Учреждения (технические и программные средства анализа, обработки, передачи и отображения, каналы информационного обмена и телекоммуникации, объекты и помещения, в которых они размещены);

4. Структура, состав и размещение средств защиты информации, их взаимодействие с информационной системой и точки подключения к ней;

5. Открытая (общедоступная) информация, необходимая для работы Учреждения, независимо от формы и вида ее представления.

2.2.2. Информационная среда Учреждения является распределенной структурой, объединяющей различные информационные системы. К основным особенностям информационной среды Учреждения относятся:

1. объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

2. важность и ответственность решений, принимаемых на основе автоматизированной обработки данных.

В этих условиях резко возрастают требования, предъявляемые к информационной среде, и в частности - к информационным системам Учреждения, в которой обрабатываются и накапливаются значительные объемы информации.

2.3. Категории информационных ресурсов, подлежащих защите

2.3.1. В информационных системах Учреждения может циркулировать информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (коммерческая или служебная тайна, персональные данные).

2.3.2. Защите подлежит вся информация, обрабатываемая в информационных системах Учреждения, независимо от ее представления и местонахождения в информационной среде, относящаяся к следующим категориям:

1. Сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом «О коммерческой тайне»;

2. Служебная информация, угроза безопасности которой может негативно повлиять на деятельность Учреждения;

3. Интересы затрагиваемых субъектов информационных отношений.

2.3.3. Субъектами информационных отношений Учреждения являются:

1. Структурные подразделения Учреждения или лица, являющиеся владельцами информационных ресурсов;

2. Подразделения Учреждения, участвующие в информационном обмене;

3. Сотрудники Учреждения, в соответствии с возложенными на них функциями;

4. Юридические и физические лица, сведения о которых присутствуют в информационной системе Учреждения;

5. Обучающиеся Учреждения;

6. Другие юридические и физические лица, прямо или косвенно задействованные в бизнес-процессах Учреждения (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

2.3.4. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

1. Своевременного доступа к необходимой информации (ее доступности);

2. Достоверности (полноты, точности, адекватности, целостности)

информации;

3. Конфиденциальности (сохранения в тайне) определенной части информации;

4. Защиты от навязывания ложной (недостоверной, искаженной) информации;

5. Ответственности за нарушения прав (интересов) и установленных правил обращения с информацией.

2.4. Цели обеспечения безопасности информации

2.4.1. Целями обеспечения безопасности информации являются:

1. Защита субъектов информационных отношений Учреждения от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;

2. Минимизация уровня рисков (утечка персональных данных, операционные риски, риск нанесения урона деловой репутации Учреждения, правовой риск и т.д.).

2.4.2. Указанные цели достигаются посредством обеспечения и постоянного поддержания следующих свойств информации:

1. Доступность информации для легальных пользователей (устойчивого функционирования информационной системы Учреждения, при котором пользователи имеют возможность своевременного получения необходимой информации);

2. Целостность и аутентичность (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой в информационной системе Учреждения;

3. Конфиденциальность определенной части информации, хранимой, обрабатываемой и передаваемой в информационной системе Учреждения.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими методами и средствами.

2.5. Задачи обеспечения безопасности информации

Для достижения целей защиты и обеспечения указанных свойств информации система информационной безопасности Учреждения должна обеспечивать эффективное решение следующих задач:

1. своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Учреждения;

2. создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

3. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и оперативная ликвидация последствий нарушения безопасности информации;

4. защита от утечки (несанкционированного разглашения и ознакомления), разрушения (несанкционированного уничтожения), блокирования (несанкционированного ограничения) или искажения (несанкционированной модификации) информации и контроль целостности используемых в информационных системах Учреждения программных средств, а также защита информационных систем от внедрения вредоносных программ;

5. защита от вмешательства в процесс функционирования информационных систем Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только авторизованные в установленном порядке пользователи);

6. разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

7. обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя

информации);

8. регистрация действий пользователей при использовании защищаемых ресурсов информационных систем Учреждения в системных журналах и периодический контроль корректности действий пользователей системы;

9. обеспечение надежности криптографических средств защиты информации.

2.6. Основные пути решения задач защиты информации

Поставленные основные цели защиты информации и решение перечисленных выше задач достигаются:

1. Строгим учетом всех подлежащих защите ресурсов информационных систем Учреждения (носителей информации, документов, каналов связи, серверов, автоматизированных рабочих мест и т.п.);

2. Регламентацией процессов обработки информации и действий пользователей;

3. Регламентацией действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

4. Полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Учреждения по вопросам обеспечения безопасности информации;

5. Назначением и подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

6. Наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Учреждения;

7. Четким знанием и строгим соблюдением всеми пользователями информационных систем Учреждения требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

8. Персональной ответственностью за свои действия каждого сотрудника, имеющего доступ к информационным ресурсам Учреждения;

9. Принятием эффективных мер обеспечения физической целостности компонентов информационной системы и непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Учреждения;

10. Применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

11. Разграничением потоков информации, предусматривающим предупреждение попадания информации более высокого уровня конфиденциальности на информационные ресурсы с более низким уровнем конфиденциальности, а также запрещением передачи конфиденциальной информации по незащищенным каналам связи;

12. Эффективным контролем над соблюдением пользователями информационных ресурсов Учреждения требований по информационной безопасности;

13. Юридической защитой интересов Учреждения при информационном взаимодействии его подразделений с внешними организациями от противоправных действий, как со стороны этих организаций и третьих лиц, так и со стороны Учреждения;

14. Проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию подсистем защиты информации информационных систем Учреждения.

2.7. Угрозы безопасности информации и их источники

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных

физических процессов техногенного характера или стихийных природных явлений, независящих от человека. Искусственные угрозы - это угрозы, вызванные деятельностью человека. Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации являются:

1. Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки, хранения и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы Учреждения, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы Учреждения;

2. Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Учреждения пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы Учреждения;

3. Деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы Учреждения в целом или ее отдельных компонент;

4. Удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

5. Ошибки, допущенные при разработке компонентов информационной

системы и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);

6. Аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации Учреждения (способами нанесения ущерба субъектам информационных отношений) являются:

1. Нарушение функциональности компонентов информационных систем Учреждения, блокирование информации, нарушение бизнес-процессов, срыв своевременного решения задач;

2. Нарушение целостности (искажение, подмена, разрушение) информационных, программных и других ресурсов;

3. Нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую или служебную тайну, а также персональных данных.

2.8. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации.

Сотрудники Учреждения, зарегистрированные как легальные пользователи информационной системы Учреждения или обслуживающие ее компоненты, могут являться внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к информационным ресурсам и процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и регламентов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации Учреждения:

– Неосторожные или халатные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;

– Разглашение, передача или утрата атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);

– Игнорирование установленных организационных правил при работе с

информационными ресурсами;

– Неквалифицированное проектирование архитектуры систем, технологий обработки данных или неквалифицированная разработка программного обеспечения, повлекшая за собой возникновение возможностей, представляющих опасность для функционирования информационной системы и безопасности информации;

– Ошибочная адресация при передаче или пересылке информации;

– Ввод ошибочных данных;

– Неумышленная порча носителей информации;

– Неумышленное повреждение каналов связи;

– Неквалифицированное (ошибочное) отключение оборудования или изменение режимов работы устройств или программ;

– Заражение компьютеров вирусами вследствие халатности пользователя;

– Неквалифицированное использование программного обеспечения, способного вызвать потерю работоспособности компонентов корпоративной информационной системы или осуществляющего необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

– Некомпетентное использование, настройка или отключение средств защиты.

2.9. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода компонентов ИС Учреждения из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

– Умышленные действия, приводящие к частичному или полному нарушению функциональности ИС Учреждения или ее компонентов, в том числе умышленное разрушение информационных или программно-технических ресурсов;

- Хищение документов и носителей информации;
- Несанкционированное копирование информации;
- Умышленное искажение информации, ввод неверных данных;
- Отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- Перехват данных, передаваемых по каналам связи;
- Хищение производственных отходов (распечаток документов, записей и т.п.);
- Незаконное получение и использование доступа к информационным ресурсам (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
- Хищение или вскрытие шифров криптозащиты информации;
- Внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов ИС Учреждения;
- Незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
- Несанкционированное применение подслушивающих устройств, фото- и видеосъемка;
- Несанкционированный перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений технических средств, непосредственно не участвующих в информационном обмене (сети питания).

2.10. Пути реализации основных естественных угроз безопасности информации

К естественным угрозам безопасности информации относятся:

- Выход из строя оборудования информационных систем и оборудования обеспечения его функционирования, не вызванный воздействиями извне и возникший по причине технической неисправности оборудования;

– Выход из строя или невозможность использования линий связи, не вызванный воздействиями извне и возникший по причине технической неисправности;

– Пожары, землетрясения, наводнения и другие стихийные бедствия.

2.11. Неформальная модель возможных нарушителей

2.11.1. Система информационной безопасности Учреждения должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

1. Некомпетентный (невнимательный) пользователь - сотрудник Учреждения (или подразделения другой организации, являющийся легальным пользователем информационной системы Учреждения), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только доступные ему штатные средства.

2. Нарушитель - сотрудник Учреждения (или подразделения другой организации, являющийся зарегистрированным пользователем информационной системы Учреждения), пытающийся нарушить систему защиты без корыстных целей или злого умысла. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.

3. Внутренний злоумышленник - сотрудник Учреждения (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов, целей вредительства или любопытства, возможно в сговоре с лицами, не являющимися сотрудниками Учреждения. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Учреждения.

4. Внешний злоумышленник - лицо, не являющееся сотрудником Учреждения, действующее целенаправленно из корыстных интересов, целей вредительства или любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Учреждения.

2.11.2. Внутренним нарушителем может быть лицо из следующих категорий:

- Зарегистрированные пользователи информационной системы Учреждения;
- Сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы Учреждения, но имеющие доступ в здание и помещения Учреждения.

2.11.3. Категории лиц, которые могут быть возможными внешними нарушителями:

- Уволенные сотрудники Учреждения;
- Представители организаций, взаимодействующих по вопросам технического обслуживания Учреждения;

- Обучающиеся в Учреждении;
- Посетители (представители организаций, поставляющих технику, программное обеспечение, услуги и т.п.);
- Лица, случайно или умышленно проникшие в информационную систему Учреждения из внешних телекоммуникационных сетей.

2.11.4. Пользователи и обслуживающий персонал из числа сотрудников Учреждения имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связаны с нарушением действующих правил и инструкций.

2.11.5. Особую категорию составляют администраторы информационных систем, имеющих практически неограниченный доступ к информационным ресурсам. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем администратора информационной безопасности.

2.11.6. Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, мерах защиты информации, правах и способах доступа к информационным ресурсам Учреждения. Полученные во время работы в Учреждения знания и опыт выделяют их среди других источников внешних угроз.

2.11.7. Профессиональные взломщики имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками Учреждения и криминальными структурами.

2.11.8. Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам.

2.11.9. Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- Нарушитель скрывает свои несанкционированные действия от других сотрудников Учреждения;

- Несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи 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 и другие средства и методы для достижения стоящих перед ним целей.

3. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.0. Построение системы безопасности информации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1. законность;
2. системность;
3. комплексность;
4. непрерывность;
5. своевременность;
6. преемственность и непрерывность совершенствования;
7. разумная достаточность (экономическая целесообразность);
8. персональная ответственность;
9. минимизация полномочий;
10. взаимодействие и сотрудничество;
11. гибкость системы защиты;
12. простота применения средств защиты;
13. обоснованность и техническая реализуемость;
14. специализация и профессионализм;
15. обязательность контроля.

3.1. Законность

Предполагает осуществление защитных мероприятий и разработку Политики информационной безопасности Учреждения в соответствии с действующим законодательством в области информации, информатизации и защиты информации, в т.ч. ПДн, других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем.

Все пользователи информационной системы Учреждения должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации Учреждения.

3.2. Системность

Системный подход к построению системы защиты информации в Учреждения предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

При создании системы защиты должны учитываться все уязвимые места информационных систем Учреждения, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

3.4. Непрерывность защиты

Обеспечение безопасности информации - постоянный процесс, осуществляемый руководством Учреждения, администратором информационной безопасности и сотрудниками всех уровней Учреждения. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности всех подразделений Учреждения.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе системы защиты информации могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

3.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

3.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы Учреждения и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного опыта в этой области.

3.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности защищаемой информации и величине возможного ущерба от ее разглашения, утраты, утечки, блокирования или искажения. Используемые

меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать функциональность компонентов информационных систем Учреждения. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности информации. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

3.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого сотрудника Учреждения в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников и степень их ответственности были четко определены.

3.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью по принципу «запрещено все, что не разрешено». Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

3.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Учреждения. В такой обстановке сотрудники должны осознанно соблюдать

установленные правила и оказывать содействие сотрудниками других отделов, обеспечивающим режим безопасности информации.

Важным элементом эффективной Политики информационной безопасности является высокая культура работы с информацией. Руководители структурных подразделений Учреждения несут ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности. Все сотрудники Учреждения должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обращения с информацией не гарантирует автоматического достижения целей защиты информации, ее отсутствие или низкий уровень создают больше возможностей для нарушения безопасности или необнаружения фактов ее нарушения.

3.11. Гибкость системы защиты

Политика информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Учреждением своей деятельности. В число таких изменений входят:

- Изменения организационной и штатной структуры Учреждения;
- Корпоративная реструктуризация, слияния и поглощения;
- Расширение деятельности;
- Изменение существующих или внедрение принципиально новых информационных систем;
- Новые технические средства;
- Новые услуги, продукты.

Свойство гибкости системы информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

3.12. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том,

что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

3.13. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

3.14. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

3.15. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться специалистами, в чьи должностные обязанности входит обеспечение безопасности информации в Учреждении.

3.16. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при

совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с обработкой, хранением и передачей информации, и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы информационной безопасности, выявленные сотрудниками Учреждения, должны своевременно доводиться до сведения руководителей соответствующего уровня и оперативно устраняться. Важно, чтобы после получения информации соответствующие руководители обеспечивали своевременное исправление недостатков. Руководство должно периодически получать отчеты, суммирующие все проблемы, выявленные системой информационной безопасности. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

4. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.0. Все меры обеспечения безопасности информационной системы Учреждения подразделяются на:

1. законодательные (правовые);
2. морально-этические;
3. технологические;
4. организационные (административные);
5. физические;
6. технические (аппаратные и программные).

4.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации, и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

4.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Учреждения. Эти нормы большей частью не являются обязательными как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Учреждения в целом. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

4.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений.

4.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

4.4.1. Формирование политики информационной безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать комплекс организационно-распорядительных документов (положений, регламентов, инструкций и т.д.), образующих Политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

4.4.2. Регламентация доступа в помещения

Особо важные компоненты информационных систем Учреждения должны размещаться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность

находящихся в помещении защищаемых ресурсов (документов, оборудования, реквизитов доступа и т.п.). Допуск в такие помещения должен производиться в присутствии ответственного, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

4.4.3. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационной системой Учреждения и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком согласно регламенту предоставления доступа пользователей.

Основными пользователями информации в информационных системах являются сотрудники Учреждения. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационным ресурсам в обязательном порядке должно согласовываться с администратором безопасности, ответственным за информационное сопровождение данного ресурса;

- руководитель имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;

- наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники Учреждения или других организаций несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы. В должностные инструкции каждого сотрудника обязательно включение задач по обеспечению информационной безопасности.

При приеме на работу сотрудники должны быть ознакомлены под роспись с перечнем информации, составляющей коммерческую или служебную тайну Учреждения, с установленным режимом работы с ней и с мерами ответственности за нарушение этого режима. Это делается в форме заключения с сотрудником отдельного соглашения о неразглашении конфиденциальной информации, действующее в период действия трудового договора и в течение трех лет с момента его прекращения.

Обработка информации в компонентах информационной системы Учреждения должна производиться в соответствии с утвержденными технологическими инструкциями.

4.4.4. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

Подлежащие защите ресурсы системы (документы и данные, оборудование, программное обеспечение) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

Ввод в эксплуатацию новых АРМ и все изменения в конфигурации существующих технических и программных средств должны осуществляться только в соответствии с утвержденными регламентами.

Все программное обеспечение (разработанное специалистами Учреждения, полученное централизованно или приобретенное у фирм-производителей) должно в установленном порядке проходить испытания. Использование нелицензионного или не прошедшего проверку программного обеспечения, должно быть запрещено.

Разработка задач (комплексов задач), проведение испытаний разработанного или приобретенного программного обеспечения, и передача его в эксплуатацию должна осуществляться в соответствии с установленным порядком разработки,

проведения испытаний и передачи задач (комплексов задач) в эксплуатацию.

4.4.5. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

На всех АРМ, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие категории данных АРМ).

Узлы и блоки вычислительной техники, доступ обслуживающего персонала к которым в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к их монтажным схемам должны закрываться и при необходимости опечатываться сотрудниками дирекции ИБ. На печати (пломбе) в обязательном порядке должна присутствовать дата пломбирования, фамилия и подпись лица, установившего ее. Печать (пломба) должна быть размещена так, чтобы вскрытие узла или блока без ее повреждения было бы невозможно.

Повседневный контроль за целостностью и соответствием печатей (пломб) на системных блоках ПЭВМ должен осуществляться пользователями и администраторами информационной системы. Периодический контроль - сотрудниками, ответственными за безопасность информации в Учреждения.

4.4.6. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем Учреждения, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации.

Все пользователи информационных систем Учреждения должны быть ознакомлены с организационно-распорядительными документами по обеспечению информационной безопасности в части их касающейся, должны знать и неукоснительно выполнять регламенты, инструкции и общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

4.4.7. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы Учреждения. Расследование/исследование нарушений

Любое грубое нарушение порядка и правил пользования информационными ресурсами Учреждения должно расследоваться. К виновным должны применяться адекватные законные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться уровнем нанесенного ущерба, наличием злого умысла и другими факторами по усмотрению руководства Учреждения.

Для реализации принципа персональной ответственности пользователей за свои действия необходима:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. закрепление за каждым пользователем персонального идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности, а также контроль за проведенными операциями в информационной системе Учреждения;
- проверка подлинности пользователей (аутентификация) на основе их идентификаторов, сертификатов, паролей, ключей, хранимых на различной физической основе, биометрических характеристик личности и т.п.;
- регистрация (протоколирование) доступа к компонентам и ресурсам информационной системы с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5. СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для обеспечения информационной безопасности в Учреждении используются следующие средства защиты информации:

1. физические средства;
2. технические средства;
3. средства управления системой информационной безопасности;
4. средства оценки эффективности систем защиты.

5.1. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информационной системы может осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих защищаемых средств, а также исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств съема (перехвата) информации.

5.2. Программные и программно-аппаратные средства защиты информации

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты могут быть

включены следующие средства:

- средства разграничения доступа к данным;
- средства криптографической защиты информации;
- средства антивирусной защиты информации;
- средства анализа защищенности.

На средства защиты информации возлагаются решение следующих основных задач:

- идентификация и аутентификация пользователей;
- управление доступом пользователей в помещения, к физическим и информационным ресурсам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защиты каналов передачи конфиденциальной информации;
- защита данных системы информационной безопасности от доступа всех пользователей, включая системных администраторов.

Зоны ответственности и задачи конкретных программных и программно-аппаратных средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

5.3. Средства управления системой информационной безопасности

Управление системой информационной безопасности представляет собой целенаправленное воздействие на компоненты системы информационной безопасности (организационные, технические, программные и криптографические) с целью достижения требуемого уровня защищенности циркулирующей в информационной системе Учреждения информации.

Главной целью организации управления системой информационной безопасности является обеспечение надежной защиты информации в процессе ее обработки, хранения и передачи.

Управление системой информационной безопасности может быть реализовано при помощи специализированной подсистемы, представляющей

собой совокупность органов управления, технических, программных и криптографических средств, организационных мероприятий и взаимодействующих друг с другом пунктов управления различных уровней.

5.4. Средства контроля эффективности системы защиты

Контроль эффективности системы защиты информации осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к информационным и другим ресурсам, блокирования, искажения, разрушения или утечки информации, а также повреждения или уничтожения компонентов информационной системы Учреждения и самой системы защиты.

Контроль может проводиться как администратором информационной безопасности Учреждения, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности применяемых в Учреждении мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

6. ТЕХНИЧЕСКАЯ ПОЛИТИКА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Реализация технической политики в области обеспечения безопасности информации должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (программно-аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической политики информационной безопасности Учреждения являются:

1. обеспечение защиты ресурсов Учреждения от повреждения или уничтожения за счет несанкционированного доступа;
2. обеспечение защиты информации от блокирования, утечки, разрушения или искажения при ее обработке, хранении и передаче по каналам связи.

Система информационной безопасности Учреждения должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, при использовании технических и программных средств.

В рамках указанных направлений технической политики информационной безопасности осуществляются:

- реализация разрешительной системы допуска пользователей и обслуживающего персонала к информационным и другим ресурсам;
- реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и

объективное документирование событий;

- ограничение доступа к ресурсам, связанным с обработкой и хранением конфиденциальной информации, а также в помещения, где проводятся работы конфиденциального характера;

- разграничение доступа пользователей и обслуживающего персонала к ресурсам Учреждения и компонентам системы защиты информации;

- учет информационных ресурсов, регистрация действий пользователей и обслуживающего персонала, контроль за доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

- предотвращение внедрения в локальную сеть Учреждения или информационную систему вредоносного программного обеспечения (вирусов, троянских коней, программных закладок и т.п.);

- реализация инфраструктуры открытого ключа, криптографическая защита конфиденциальной информации, передаваемой по открытым каналам связи;

- надежное хранение документов и носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;

- необходимое резервирование технических средств и носителей информации, в т.ч. ПДн.

7. ФОРМИРОВАНИЕ РЕЖИМА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

7.1. С учетом выявленных угроз безопасности информации, режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в информационной среде Учреждения информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации.

7.2. Комплекс мер по формированию режима обеспечения безопасности информации включает:

1. установление организационно-правового режима обеспечения безопасности информации (разработку необходимых нормативных

документов, работа с персоналом, правил делопроизводства);

2. выполнение организационно-технических мероприятий по защите конфиденциальной информации от утечки;
3. организационные и программно-технические мероприятия по предупреждению несанкционированных действий с информационными ресурсами Учреждения;
4. комплекс мероприятий по контролю функционирования информационных систем Учреждения после случайных или преднамеренных воздействий;
5. комплекс оперативных мероприятий администратора безопасности по предотвращению (выявлению) проникновения на территорию и в помещения лиц, имеющих отношение к криминальным структурам.

7.3. Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку и введение в действие следующих организационно-распорядительных документов:

1. политика в отношении обработки и защиты персональных данных;
2. положение по организации обработки персональных данных;
3. перечень информации, подлежащей защите;
4. инструкции и функциональные обязанности сотрудников;
5. другие нормативные документы, входящие в состав Политики информационной безопасности.

7.4. Организационно-технические мероприятия по защите конфиденциальной информации от утечки предусматривают:

1. комплекс мер и соответствующих технических средств, предотвращающих или ослабляющих утечку информации (пассивная защита);
2. комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации (поиск и обнаружение).

7.5. Физическая охрана компонентов информационной системы Учреждения включает:

1. организацию системы охранно-пропускного режима и системы контроля допуска на объект;

2. введение дополнительных ограничений по доступу в помещение, предназначенные для хранения и обработки конфиденциальной информации (кодовые и электронные замки, карточки допуска и т.д.);

3. визуальный и технический контроль контролируемой зоны объекта защиты;

4. применение систем охранной и пожарной сигнализации.

7.6. Выполнение режимных требований при работе с конфиденциальной информацией предполагает:

1. разграничение допуска к ресурсам информационных систем Учреждения;

2. ведение учета ознакомления сотрудников с конфиденциальной информацией;

3. заключение с сотрудниками отдельного соглашения о неразглашении ставшей им доступной конфиденциальной информации;

4. организация уничтожения информационных отходов (бумажных, магнитных, оптических и т.д.);

5. оборудование служебных помещений сейфами, шкафами для хранения носителей информации.

7.7. Мероприятия технического контроля предусматривают:

1. контроль за проведением технического обслуживания, ремонта носителей информации и средств вычислительной техники;

2. проверки поступающего оборудования, предназначенного для обработки конфиденциальной информации, на наличие специально внедренных закладных программ и устройств;

3. оборудование компонентов информационной системы устройствами защиты от сбоев электропитания и помех в линиях связи;

4. защита выделенных помещений при проведении закрытых работ (переговоров);

5. постоянное обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствии с меняющейся оперативной обстановкой.

8. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ


Реализация Концепции информационной безопасности в Учреждении позволит:

1. оценить состояние безопасности информации в Учреждении, выявить источники внутренних и внешних угроз ИБ, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
2. разработать распорядительные и нормативно-методические документы, применительно к ИС;
3. провести организационно-режимные и технические мероприятия по обеспечению безопасности информации в ИС;
4. обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы защиты информации в Учреждении и создаст условия для её дальнейшего совершенствования.

РАЗРАБОТАНО:

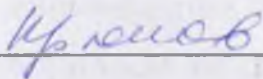
Ведущий специалист по
кадрам



Т.О.Медяшкина

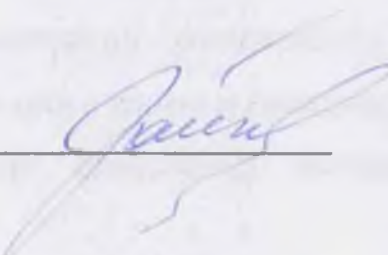
СОГЛАСОВАНО:

Заместитель директора по
учебно
производственной работе



С.А. Крюков

Юрисконсульт



Э.Н. Зайкова

9. ИСТОРИЯ ИЗМЕНЕНИЙ

№	Дата	Версия	Предмет изменений	Автор
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				