

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная
безопасность систем и технологий»

Специальность 100503 –

Информационная безопасность
автоматизированных систем

Специализация -

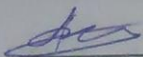
Защищенные
автоматизированные системы
управления

ДИПЛОМНАЯ РАБОТА

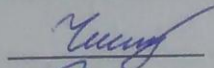
на тему

МЕТОДИКА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ
РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ХОДЕ ПРОВЕДЕНИЯ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ОПЫТНО-КОНСТРУКТОРСКИХ
РАБОТ НА ПРЕДПРИЯТИИ АО «ПНИЭИ»

Студент

 Борисов Андрей Евгеньевич

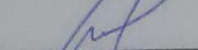
Руководитель

 Чистова М.С.

Нормоконтролёр

 Иванов А.П.

Рецензент ведущий инженер АО «ПНИЭИ»

 Логинов К.Е.

Работа допущена к защите (протокол заседания кафедры от 10.06.2016 № 14)

Заведующий кафедрой

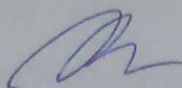
 С.Л. Зефилов

Работа защищена с отметкой удовл.

(протокол заседания ГЭК

от 23.06.16 № 2)

Секретарь ГЭК

 А.П. Иванов

РЕФЕРАТ

Пояснительная записка содержит 80 с., 3 рис., 27 табл., источников, 1 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ, ЗАЩИТА ИНФОРМАЦИИ, АКТИВЫ ОРГАНИЗАЦИИ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА, УГРОЗА, УЯЗВИМОСТЬ, РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ЗАЩИТНЫЕ МЕРЫ

Объектом дипломной работы является методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Цель дипломной работы - разработка методики защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

В процессе дипломной работы осуществляется анализ проблемы защиты конфиденциальной информации, разрабатывается структура и модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения, производится идентификация и оценка ценности активов, анализ и оценка угроз информационной безопасности, разрабатывается модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения, проводится анализ и оценка уязвимостей активов автоматизированной системы, анализ и оценивание рисков, определение способов обработки рисков информационной безопасности, а также осуществляется выбор мер по защите конфиденциальной информации.

В результате дипломной работы разработана методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

СОДЕРЖАНИЕ

Введение	7
1 Анализ проблемы защиты конфиденциальной информации.....	8
2 Структура автоматизированной системы отделов по разработке программного обеспечения	15
3 Модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения	18
4 Идентификация и оценка ценности активов	20
5 Анализ и оценка угроз информационной безопасности	24
6 Модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения	33
7 Анализ и оценка уязвимостей активов автоматизированной системы.....	41
8 Анализ рисков информационной безопасности	45
9 Оценивание рисков информационной безопасности	47
10 Определение способов обработки рисков информационной безопасности.....	54
11 Выбор мер по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии.	56
Заключение	61
Список использованных источников	62
Приложение А (обязательное).....	63

ОПРЕДЕЛЕНИЯ

В настоящей выпускной квалификационной работе применяют следующие термины с соответствующими определениями:

– информационная безопасность – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1];

– конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации [2];

– защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных непреднамеренных воздействий на защищаемую информацию [3];

– активы организации – все что имеет ценность для организации в интересах достижения целей деятельности и находится в её распоряжении (информационные активы, ресурсы, процессы, выпускаемая продукция) [4];

– автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [5];

– угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [3];

– уязвимость – свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации [3];

– риск информационной безопасности – это способность конкретной угрозы использовать уязвимости одного или нескольких видов активов для нанесения ущерба организациях [6].

– защитные меры – это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость,

ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов [6].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей выпускной квалификационной работе применяют следующие обозначения и сокращения:

- АС – автоматизированная система;
- АО – акционерное общество;
- АРМ – автоматизированное рабочее место;
- АСУ – автоматизированная система управления;
- БД – база данных;
- ВА – вспомогательный актив;
- ИБ – информационная безопасность;
- ИС – информационная система
- НИОКР – научно-исследовательские опытно-конструкторские работы;
- ПО – программное обеспечение
- СВТ – средство вычислительной техники.

ВВЕДЕНИЕ

Актуальность защиты конфиденциальной информации связана с ростом возможностей вычислительной техники и возможностями утечки этой информации. Развитие средств, методов обработки информации, массовое применение ЭВМ повышают уязвимость информации.

Целью работы является разработка методики защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Разрабатываемая методика предназначена для использования в отделах предприятия АО «ПНИЭИ» по разработке программного обеспечения.

В ходе выполнения дипломной работы осуществляется:

- анализ проблемы защиты конфиденциальной информации;
- структура автоматизированной системы отделов по разработке программного обеспечения;
- модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения;
- идентификация и оценка ценности активов;
- анализ и оценка угроз информационной безопасности;
- модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения;
- анализ и оценка уязвимостей активов автоматизированной системы;
- анализ рисков информационной безопасности;
- оценивание рисков информационной безопасности;
- определение способов обработки рисков информационной безопасности;
- выбор мер по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии.

1 Анализ проблемы защиты конфиденциальной информации

В настоящее время автоматизированные системы являются основой обеспечения практически любых бизнес-процессов как в коммерческих, так и в государственных организациях. Вместе с тем использование АС для хранения, обработки и передачи информации приводит к проблемам, связанных с их защитой.

Одна из основных проблем обработки конфиденциальных документов – это утрата информационных ресурсов ограниченного доступа, которая может быть осуществлена конкурирующими с организацией учреждениями или фирмами. Среди внутренних угроз безопасности информации можно выделить:

- нарушение конфиденциальности информации;
- искажение информации;
- утрата информации;
- сбои в работе оборудования и информационных систем;
- кража оборудования.

Риск утечки информации определяется ценностью этой информации для организации и вероятности утечки.

Ценность информации, при угрозе её утечки, определяется на основании таких критериев, как:

- последствия для бизнеса, включая ущерб неосязаемых активов и потерю конкурентоспособности;
- затрата времени и ресурсов и на восстановление информации;
- юридические последствия, ответственность и иски, штрафы и санкции, отзыв лицензий;
- актуальность информации, влияние времени на ее ценность.

Основными источниками конфиденциальной информации являются:

- персонал предприятия, допущенный к КИ;
- носители конфиденциальной информации (документы, изделия);

- технические средства, предназначенные для хранения и обработки информации;
- передаваемые сообщения, содержащие конфиденциальную информацию.

Способы обмена конфиденциальной информацией в организации могут носить как непосредственный характер, так и характер передачи информационных сообщений с помощью технических средств и систем связи.

Из существующих способов обмена конфиденциальной информацией необходимо выделить организационные каналы передачи и обмена информацией:

- защищенный документооборот;
- совместные работы, выполняемые предприятием по направлениям его производственной и иной деятельности;
- совещания (конференции), в ходе проведения которых могут обсуждаются вопросы конфиденциального характера;
- научные исследования, деятельность научно – исследовательские работы;
- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты несанкционированному воздействию со стороны злоумышленников, целью которого будет являться получение и использование этой информации.

Данное воздействие, в свою очередь, приведет к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на предотвращение утечки и несанкционированного распространения конфиденциальной информации (утраты носителей конфиденциальной информации).

Для предотвращения утечки конфиденциальной информации с помощью СВТ необходима техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащих защите с применением технических, программных и программно-технических средств.

Разнообразие технических средств защиты информации огромно. К средствам технической защиты информации, помимо средств контроля, относятся также средства защиты информации от непреднамеренного уничтожения или искажения. Примеры технических средств защиты информации:

Программные средства – специальные программы и программные комплексы, предназначенные для защиты информации в ИС, (антивирусы, файрволы; системы обнаружения сетевых атак; системы разграничения доступа к данным и т.д.).

Программно-аппаратные средства – это сервисы безопасности, встроенные в ОС (маршрутизаторы и файрволы Cisco, Juniper и т.п.; комплексные решения по обнаружению сетевых аномалий; системы предотвращения утечек данных; комплекты резервного копирования и архивирования данных, и другие.)

Аппаратные средства – устройства, встраиваемые непосредственно в ВТ, или устройства, которые сопрягаются с ней по стандартному интерфейсу (устройства обнаружения закладных устройств; сканеры радиоизлучения; генераторы радиопомех и другие.)

Решение проблем защиты конфиденциальной информации на электронных носителях базируется, в том числе и на использовании криптографических методов. Алгоритм заключается в следующем:

Отправитель сообщения выполняет шифрование, получатели выполняют обратное преобразование – расшифровку. Ключевая информация (ключи шифрования) либо доставляется по защищенному каналу связи, либо совместно генерируется участниками. Злоумышленник, если он контролирует среду, по

которой передается сообщение, даже в случае полного перехвата не сможет ознакомиться с его содержанием.

Современные методы криптографического преобразования сохраняют исходную производительность автоматизированной системы, что является немаловажным. Это является наиболее эффективным способом, обеспечивающим конфиденциальность данных, их целостность и подлинность. Использование криптографических методов в совокупности с техническими и организационными мероприятиями обеспечивают надежную защиту от широкого спектра угроз.

Несанкционированная модификация информации - внесение в информацию каких-либо изменений в интересах злоумышленника. Несанкционированная модификация информации может нанести ущерб владельцу информации и (или) организации и принести злоумышленнику выгоду. Из несанкционированной модификации информации можно выделить следующую угрозу, такую как создание ложных сообщений. Это означает, что злоумышленник преднамеренно посылает субъекту заведомо ложную информацию, получение и использование которой данным субъектом выгодно злоумышленнику. При этом передаваемая информация полностью соответствует всем атрибутам и реквизитам, которые не позволяют получателю заподозрить, что эта информация ложная.

Блокирование доступа к информации или ресурсам системы может иметь негативные последствия в, случае, когда некоторая информация обладает реальной ценностью только на протяжении короткого отрезка времени. В этом случае блокирование нарушает требование своевременности получения информации. Также блокирование доступа к информации может привести к тому, что субъект не будет обладать всей полнотой сведений, необходимых для принятия решения. Одним из способов блокирования информации может быть отказ в обслуживании, когда система вследствие сбоев в работе или действий злоумышленника не отвечает на запросы санкционированного пользователя.

Несанкционированное или ошибочное использование ресурсов системы, с одной стороны, может служить промежуточным звеном для уничтожения, модификации или распространения информации. С другой стороны, оно имеет самостоятельное значение, так как, даже не касаясь пользовательской или системной информации, может нанести ущерб самой системе (например, вывести ее из строя).

Отказ от получения или отправки информации заключается в отрицании пользователем факта посылки или приема какого-либо сообщения. Например, при осуществлении банковской деятельности подобные действия позволяют одной из сторон расторгать так называемым "техническим" путем заключенные финансовые соглашения, т. е. формально не отказываясь от них. Это может нанести второй стороне значительный ущерб.

Перечисленные виды угроз могут реализовываться различными способами, которые зависят от источника и вида угрозы. Существует большое количество подобных способов (особенно в сфере безопасности компьютерных сетей), они постоянно совершенствуются и обновляются.

«Одним из примеров, нуждающихся в защите конфиденциальной информации является конфиденциальная информация, используемая при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ». АО «ПНИЭИ» - одно из крупнейших предприятий России, занимающееся разработкой и производством техники криптографической защиты информации, телекоммуникационного оборудования для сетей специальной связи министерств и ведомств, финансово-кредитных структур, предприятий и организаций любой формы собственности.

Основными целями деятельности АО «ПНИЭИ» являются:

- извлечение прибыли;
- участие в реализации государственных программ;
- иные цели, не запрещенные законодательством Российской Федерации.

Для достижения целей предприятие осуществляет в установленном Российской Федерации порядке следующие виды деятельности:

- обеспечение конфиденциальности, достоверности, целостности информации при передаче ее по различным каналам связи;
- разработка комплексов и технических средств криптографической защиты информации;
- разработка средств специальной связи;
- разработка аппаратуры по требованиям Заказчика;
- проектирование защищенных информационных систем;
- создание комплексных решений в области безопасности информационных и управляющих систем;
- создание средств управления защищенными информационно-телекоммуникационными сетями;
- создание специальных систем передачи данных;
- создание средств электронного документооборота;
- развитие и внедрение биометрико-нейросетевых технологий;
- обеспечение передачи сигналов по каналам низкого качества в условиях воздействия помех;
- серийное производство технических средств криптографической защиты информации и средств специальной связи;
- аттестация технических средств защиты информации и объектов информатизации по требованиям безопасности ФСТЭК России;
- аттестация помещений и объектов информатизации на право обработки информации, составляющей коммерческую и (или) государственную тайну;
- сертификационные испытания технических средств обработки и защиты информации в системе сертификации Минобороны России;
- сертификационные испытания средств криптографической защиты информации в системе сертификации ФСБ России;

— специальные исследования технических средств и систем, обрабатывающих информацию, составляющую государственную или коммерческую тайну»[8]

При рассмотрении данной организации, в частности, взаимодействия отделов по разработке программного обеспечения, была сформулирована цель функционирования (бизнес-цель): разработка и усовершенствование программного обеспечения.

2 Структура автоматизированной системы отделов по разработке программного обеспечения

Графическое изображение процесса «Разработка и усовершенствование программного обеспечения» приведено на рисунке 1.

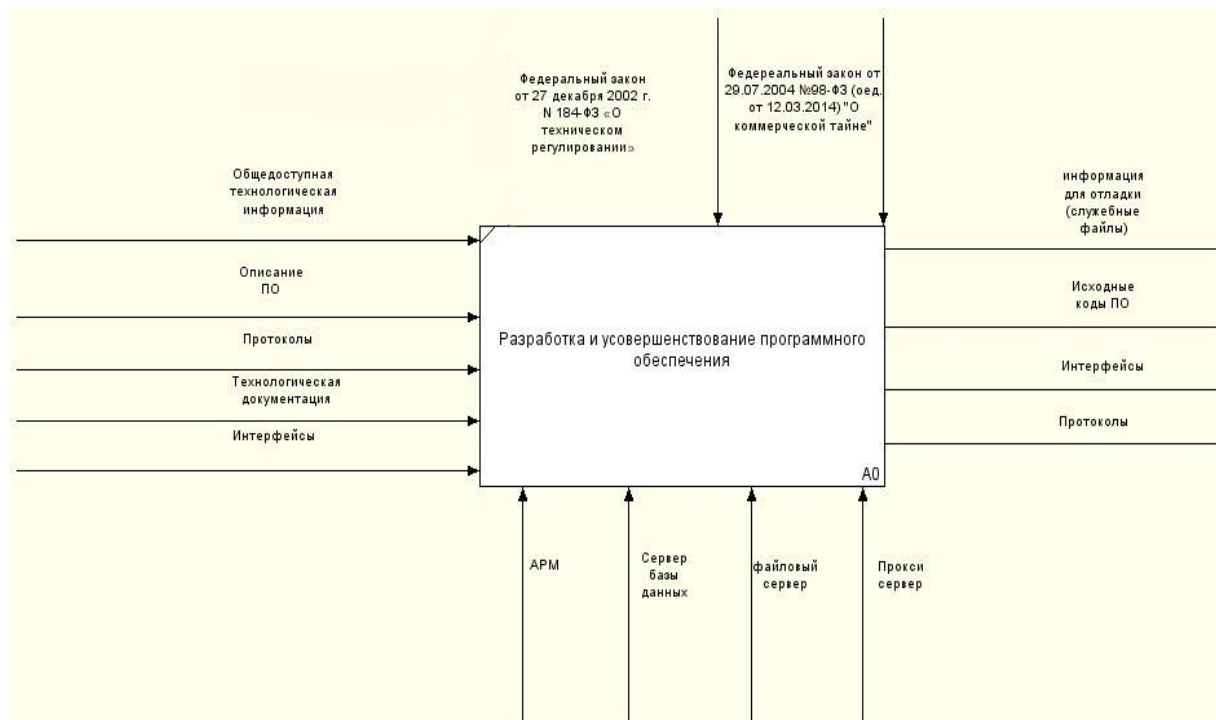


Рисунок 1 - Графическое изображение процесса «Разработка и усовершенствование программного обеспечения»

Входными данными являются:

- Общедоступная технологическая информация;
- Описание ПО;
- Протоколы;
- Технологическая документация;
- Интерфейсы.

Выходными данными являются:

- Информация для отладки;
- Исходные коды ПО;
- Интерфейсы;
- Протоколы.

Ресурсами являются:

- АРМ инженеров-программистов;
- Сервер БД;
- Файловый сервер;
- Прокси сервер.

Управление осуществляется:

- Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне";
- Федеральный закон от 27 декабря 2002 №184-ФЗ «О техническом регулировании»

ИС взаимодействия отделов по разработке программного обеспечения состоит из следующих элементов:

- автоматизированные рабочие места (АРМ) инженеров-программистов;
- сервер базы данных;
- файловый сервер;
- прокси сервер.

Далее была составлена структура отделов по разработке программного обеспечения, представленная на рисунке 2.

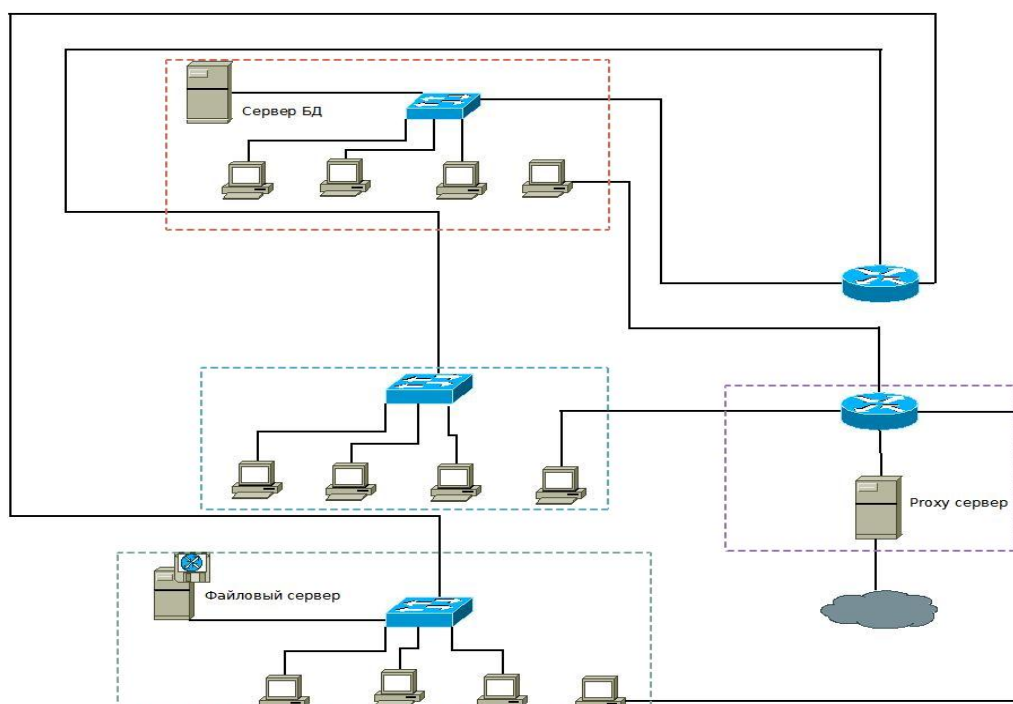


Рисунок 2 — Структура отделов по разработке ПО

Из данной структуры (см. рисунок 2) видно, что АРМ отделов занимающихся разработкой ПО, находятся в разных подсетях. Для связи АРМ друг с другом в пределах одного отдела компьютеры подключены к коммутатору. Для автоматизации работы отделов все подсети соединены между собой при помощи маршрутизатора. Для получения информации из сети Internet в каждом из отделов предусмотрены по одному АРМ, который не связан с остальными компьютерами в отделе.

3 Модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения

Далее была построена инфологическая модель отделов по разработке ПО, представляющая собой направленный граф. Инфологическая модель представлена на рисунке 3. Ребрами графа являются информационные потоки, связывающие информационные компоненты. Направление ребер определяет направление информационного потока.

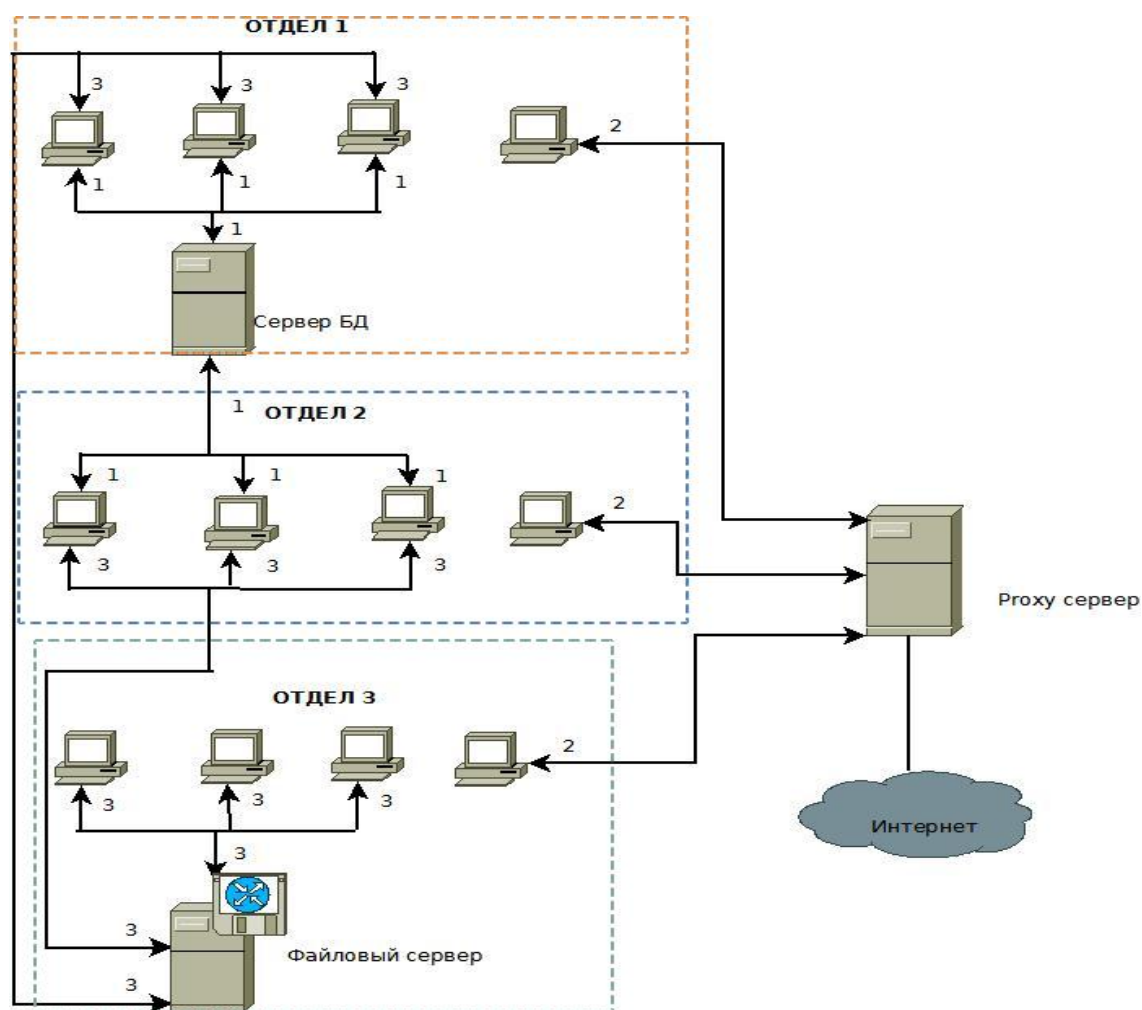


Рисунок 3 - Инфологическая модель отделов по разработке ПО

В данной организации существуют следующие типы информации:

- 1 - конфиденциальная информация: информация для отладки (служебные файлы)
- 2 - общедоступная технологическая информация;

– 3 - конфиденциальная информация: исходные коды ПО, программная документация (описание ПО, протоколы, интерфейсы, технологическая документация).

Ребрами графа являются информационные потоки, связывающие информационные компоненты. Направление ребер определяет направление информационного потока.

Для каждого ребра указывается степень конфиденциальности информации

Файловый сервер обеспечивает бесперебойное получение информации при запросе на ее получение, а также добавление новых файлов, необходимых для выполнения дальнейших работ. Доступ к исходным кодам, программной документации, хранящимся на файловом сервере имеют все отделы по разработке ПО.

Сервер БД также отвечает за целостность и сохранность данных, а также обеспечивает операции клиента к информации. Доступ к служебным файлам, хранящимся на сервере БД может осуществляться с АРМ 1 и 2 отделов.

Для получения информации из Internet используется Proxy сервер. Он используется для защиты локальной сети от внешнего доступа, а также защиты локальной сети от внешнего доступа.

4 Идентификация и оценка ценности активов

Для проведения оценки рисков ИБ организации были идентифицированы информационные активы (ИА) организации и определены значимые свойства ИБ для каждого из них. Информационными активами будут являться:

- информация для отладки (служебные файлы);
- общедоступная технологическая информация;
- исходные коды ПО;
- описание ПО;
- протоколы;
- интерфейсы;
- технологическая документация.

Вспомогательными активами будут являться:

- АРМ инженеров-программистов;
- файловый сервер;
- сервер БД;
- прокси сервер.

Результаты идентификации информационных активов приведены в таблице 1.

Таблица 1 - Перечень информационных активов и их значимые свойства ИБ

Информационный актив	Значимые свойства ИБ			
	Конфиденциальность	Целостность	Доступность	Неотказуемость
[ИА1] информация для отладки (служебные файлы);	+	+	+	—
[ИА2] общедоступная технологическая информация;	—	+	+	—

Продолжение таблицы 1

Информационный актив	Значимые свойства ИБ			
	Конфиденциальность	Целостность	Доступность	Неотказуемость
[ИА3]Исходные коды ПО	+	+	+	+
[ИА4]описание ПО	+	+	+	—
[ИА5]протоколы,	—	+	+	—
[ИА6]интерфейсы,	—	—	+	—
[ИА7]технологическая документация	—	+	+	+

Для каждого значимого свойства каждого ИА была определена величина нарушения ИБ в соответствии со следующей качественной шкалой:

- минимальная (1);
- средняя (2);
- высокая (3);
- критическая (4).

Величина потенциального ущерба от нарушения свойств ИБ активов была оценена по следующим направлениям:

- степень влияния на непрерывность деятельности организации;
- объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;
- объем дополнительных людских ресурсов, необходимых для восстановления свойств ИБ для ИА и ликвидации последствий нарушения ИБ;
- объем дополнительных временных затрат, необходимых для восстановления свойств ИБ для ИА и ликвидации последствий нарушения ИБ;
- степень нарушения законодательных требований и (или) договорных обязательств организации.

Результаты оценивания величины нарушений ИБ для каждого информационного актива (ИА) по направлениям приведены в таблице 2.

Таблица 2 - Определение ценности основных (информационных) активов

Информационный актив	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщённая величина нарушения ИБ	Ценность актива
		1	2	3	4	5		
[ИА1] информация для отладки (служебные файлы);	Конфиденциальность	4	4	5	4	5	5	5
	Целостность	4	3	4	5	5	5	
	Доступность	4	4	3	4	4	4	
[ИА2] общедоступная технологическая информация;	Конфиденциальность	2	2	2	1	2	2	2
	Целостность	2	2	2	2	2	2	
	Доступность	2	1	2	2	1	2	
[ИА3] Исходные коды ПО	Конфиденциальность	3	3	4	3	4	4	4
	Целостность	3	3	3	4	4	4	
	Доступность	3	2	3	2	3	3	
	Неотказуемость	2	3	3	4	2	3	
[ИА4] описание ПО	Конфиденциальность	3	3	3	3	3	3	3
	Целостность	3	2	2	2	2	2	
	Доступность	3	2	3	2	3	3	
[ИА5] протоколы	Конфиденциальность	2	2	1	2	3	2	2
	Целостность	2	2	2	2	2	2	
	Доступность	2	1	2	2	2	2	
[ИА6] интерфейсы	Конфиденциальность	3	2	3	2	3	3	3
	Целостность	3	3	2	3	3	3	
	Доступность	2	2	3	3	3	3	
[ИА7] технологическая документация	Конфиденциальность						4	4
		3	3	4	3	4		
	Целостность						4	
		3	3	3	4	4		
	Доступность						3	
		3	3	3	3	4		

Результаты оценки ценности вспомогательных активов (ВА) с учетом зависимостей между вспомогательными и информационными активами представлены в таблице 3.

Таблица 3 – Перечень вспомогательных активов и их значимые свойства

Вспомогательный актив	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива
		Актив	Ценность актива	
[BA1]АРМ Инженеров - программистов	3	ИА1	5	5
		ИА3	2	
		ИА4	3	
		ИА5	2	
		ИА6	3	
		ИА7	4	
[BA2]Файловый сервер	4	ИА3	4	4
		ИА4	3	
		ИА5	2	
		ИА6	3	
		ИА7	4	
[BA3]Сервер БД	4	ИА1	5	5
[BA4] Прокси сервер	3	ИА2	2	3

Таким образом, наиболее ценными активами АС отделов по разработке программного обеспечения являются следующие:

- информация для отладки (служебные файлы);
- АРМ инженеров-программистов;
- сервер БД;
- исходные коды ПО;
- технологическая документация;
- файловый сервер.

5 Анализ и оценка угроз информационной безопасности

При исследовании ИС АО ПНИЭИ были выделены следующие угрозы ИБ:

- утечка информации по техническим каналам;
- противоправные сбор и использование информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- нарушения технологии обработки информации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Описание угроз ИБ представлено в таблице 4.

Таблица 4 – Описание угроз

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия
1	Утечка информации по техническим каналам	Лица, не имеющие доступа к АСУ	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на АРМ Информация, обрабатываемая на серверах ; Информация, передаваемая через подсистемы передачи информации

Продолжение таблицы 4

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия
2	Противоправные сбор и использование информации	Лица, не имеющие доступа к АСУ	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на серверах АСУ ;
3	Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации	Персонал, имеющий доступ к защищаемой информации	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на АРМ АСУ; Информация, обрабатываемая на серверах АСУ ;
4	Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия	Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на АРМ ; Информация, обрабатываемая на серверах АСУ;

Продолжение таблицы 4

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия
5	Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи	Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации	Целостность; Доступность	Информация, обрабатываемая на АРМ АСУ ; Информация, обрабатываемая на серверах АСУ ;
6	Нарушения технологии обработки информации	Персонал, имеющий доступ к защищаемой информации	Целостность; Доступность	Информация, обрабатываемая на АРМ АСУ ; Информация, обрабатываемая на серверах АСУ ; Информация, содержащаяся на электронном или бумажном носителе информации
7	Несанкционированный доступ к информации, находящейся в банках и базах данных	Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на АРМ АСУ; Информация, обрабатываемая на серверах АСУ ; Информация, содержащаяся на электронном или бумажном носителе информации; Информация, передаваемая через подсистемы передачи информации

Продолжение таблицы 4

№ п/ п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия
8	Нарушение законных ограничений на распространение информации	Персонал, имеющий доступ к защищаемой информации	Конфиденциальность; Целостность; Доступность	Информация, обрабатываемая на АРМ АСУ ; Информация, обрабатываемая на серверах АСУ ; Информация, содержащаяся на электронном или бумажном носителе информации; Информация, передаваемая через подсистемы передачи информации

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала:

- Н — низкая вероятность. Маловероятно что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п, которые указывали бы на то, что это может произойти. Ожидаемая частота реализации угрозы не превышает одного раза в 5-10 лет;
- С — средняя вероятность. Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий. Ожидаемая частота реализации — примерно раз в год;
- В — высокая вероятность. Эта угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия.

Ожидаемая частота реализации угрозы еженедельно или чаще.

Некоторые угрозы могут использоваться для поражения одного или нескольких активов. В таком случае угрозы могут нанести вред в зависимости от того, какие активы были повреждены.

После идентификации всех возможных угроз безопасности информации, необходимо выбрать наиболее актуальные из них. Актуальной считается угроза, которая может быть реализована в АСУ и представляет опасность для информации.

Для этого необходимо определить вероятности реализации всех угроз и их показатели опасности. Затем, на основании правила отнесения угрозы к актуальной, сделать вывод. Определение актуальности угроз приведено в таблице 5.

Таблица 5 – Определение актуальности угроз

Угроза	Вероятность	Возможность	Опасность	Актуальность
Утечка информации по техническим каналам	4	Высокая	Средняя	Актуальна
Противоправные сбор и использование информации	1	Высокая	Высокая	Актуальна
Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации	5	Средняя	Высокая	Актуальна

Продолжение таблицы 5

Угроза	Вероятность	Возможность	Опасность	Актуальность
Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия	2	Средняя	средняя	Неактуальна
Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи	1	низкая	средняя	Неактуальна
Нарушения технологии обработки информации	2	средняя	высокая	Актуальна
Несанкционированный доступ к информации, находящейся в банках и базах данных	1	средняя	высокая	Актуальна
Нарушение законных ограничений на распространение информации	2	средняя	высокая	Актуальна

На основе составленных перечней активов организации и примеров угроз была проведена идентификация угроз информационной безопасности организации, включая определение событий, установление источника угроз, цели угрозы и типа потери. Результаты идентификации угроз приведены в таблице 6. Обозначения информационных активов (ИА) и вспомогательных

активов (ВА) соответствуют обозначениям, приведенным в таблицах 1 и 3

Графа «Тип событий» содержит следующие обозначения событий:

- У — умышленные, преднамеренные события;
- С — случайные события;
- П — события среды.

Графа «Тип потери» содержит следующие обозначения свойств ИБ:

- К — конфиденциальность;
- Ц — целостность;
- Д — доступность;
- Н — неотказуемость;
- А — аутентичность.

Таблица 6 - Описание угроз ИБ

Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
[У1] утечка информации по техническим каналам	у	Лица, не имеющие доступа к АСУ	ИА1-7,	К
[У2] противоправные сбор и использование информации	у	Персонал, имеющий доступ к защищаемой информации.	ИА1,3-7 ВА1-4	К
[У3] разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации	у	Персонал, имеющий доступ к защищаемой информации.	ИА1-3,5-7 ВА1-4	Ц, Д,Н

Продолжение таблицы 6

Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
[У4] внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия	У	Персонал, имеющий доступ к защищаемой информации.	ИА1-7	К, Ц, Д
[У5] уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи	У	Персонал, имеющий доступ к защищаемой информации.	ИА1-4 ВА1-4	Ц,Д,Н
[У6] нарушения технологии обработки информации	С,У	Персонал, имеющий доступ к защищаемой информации.	ИА1-7	Ц,Д
[У7] несанкционированный доступ к информации, находящейся в банках и базах данных	У	Персонал, имеющий доступ в КЗ, но не имеющий доступа к конфиденциальной информации.	ИА1-3,6 ВА1-4	К,Д,Ц

Продолжение таблицы 6

Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
[У8] нарушение законных ограничений на распространение информации	С,У	Персонал, имеющий доступ к защищаемой информации Бывшие сотрудники организации	ИА1,3,7	К

Таким образом, наиболее актуальными угрозами являются следующие:

- утечка информации по техническим каналам;
- противоправные сбор и использование информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации
- нарушения технологии обработки информации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

6 Модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения

На основе результатов проделанной работы была составлена модель актуальных угроз АСУ.

Описание каждой угрозы включает:

- нападения пригодные для реализации угрозы (возможность, методы, уязвимости);
- объекты нападений (объекты защиты);
- тип потери;
- масштаб ущерба;
- источники угрозы.

Сформирована следующая модель угроз:

Первая угроза - Утечка информации по техническим каналам.

Методом нападения, которым осуществляется данная угроза, являются информационно-технические воздействия.

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - средний;
- риск потери производительности – низкий;
- риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как средний.

Источники угроз: Лица, не имеющие доступа к АСУ .

Вторая угроза - Противоправные сбор и использование информации.

Методами нападения, которыми осуществляется данная угроза, являются информационно-технические воздействия с применением программно-аппаратных и программных средств (в том числе программно-математических

воздействий).

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи; отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - высокий;
- риск потери производительности - высокий;
- риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Лица, не имеющие доступа к АСУ.

Третья угроза - Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации

Методами нападения, которыми осуществляется данная угроза, являются информационно-технические воздействия с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - высокий;
- риск потери производительности - высокий;

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Четвертая угроза - Нарушения технологии обработки информации.

Методами нападения, которыми осуществляется данная угроза, являются несанкционированные действия с защищаемой информацией.

Данные методы используют следующие уязвимости: дефицит квалифицированных кадров.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - высокий;
- риск потери производительности - высокий;
- риск затруднения деятельности - средний.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Пятая угроза - Несанкционированный доступ к информации, находящейся в банках и базах данных.

Методом нападения, которым осуществляется данная угроза, является несанкционированный доступ к защищаемой информации.

Данный метод использует следующие уязвимости: несовершенства средств защиты информации и систем связи; отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - высокий;
- риск потери производительности - высокий;
- риск затруднения деятельности - средний.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации.

Шестая угроза - Нарушение законных ограничений на распространение информации.

Методами нападения, которыми осуществляется данная угроза, являются несанкционированные действия с защищаемой информацией.

Данный метод использует следующие уязвимости: несовершенства средств защиты информации и систем связи; дефицит квалифицированных кадров.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - высокий;
- риск потери производительности - высокий;
- риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Модель нарушителя ИБ

Всех потенциальных нарушителей можно подразделить на:

- внешних нарушителей, осуществляющих атаки из за пределов контролируемой зоны;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

Внутренние нарушители:

В качестве потенциальных внутренних нарушителей АО «ПНИЭИ» рассматриваются:

- зарегистрированные пользователи ИС предприятия;
- сотрудники предприятия, являющиеся сотрудниками, не допущенные к информационным ресурсам, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства;
- сотрудники структурных подразделений, обеспечивающие безопасность на предприятии;
- сотрудники, задействованные в разработке и сопровождении программного обеспечения;
- руководители различных уровней.

Внешние нарушители.

В качестве потенциальных внешних нарушителей АО «ПНИЭИ» рассматриваются:

- бывшие сотрудники предприятия;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго- , водо-, теплоснабжения и т.п.);
- посетители (приглашенные по какому либо поводу);
- лица, случайно или умышленно нарушившие пропускной режим;
- конкурирующие с предприятием организации;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

– лица, случайно или умышленно проникшие в ИС из внешней сети (хакеры).

Цели, преследуемые нарушителями, могут быть следующие:

- сбор информации;
- финансовая выгода;
- конкурентная выгода;
- месть;
- любопытство.

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

- нарушитель скрывает свои действия от других сотрудников;
- внутренний и внешний нарушитель могут быть в сговоре;
- в своей деятельности нарушитель может использовать любое средство для перехвата информации, воздействия на информацию и другие средства для достижения поставленных перед ним целей.

Далее на основании выявленных угроз и нарушителей была составлена таблица угроз — нарушитель.

Таблица 7 — Угроза - нарушитель

Угроза	Нарушитель
Утечка информации по техническим каналам	<ul style="list-style-type: none">- сотрудники предприятия, являющиеся сотрудниками, не допущенные к информационным ресурсам, но имеющие доступ в здания и помещения;- персонал, обслуживающий технические средства;- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго- , водо- - теплоснабжения и т.п.);

Продолжение таблицы 7

Угроза	Нарушитель
Противоправные сбор и использование информации	<ul style="list-style-type: none"> - зарегистрированные пользователи ИС предприятия; - персонал, обслуживающий технические средства; - сотрудники предприятия, являющиеся сотрудниками, не допущенные к информационным ресурсам, но имеющие доступ в здания и помещения; - сотрудники, задействованные в разработке и сопровождении программного обеспечения; - лица, случайно или умышленно проникшие в ИС из внешней сети (хакеры);
Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации	<ul style="list-style-type: none"> - сотрудники, задействованные в разработке и сопровождении программного обеспечения; - персонал, обслуживающий технические средства; - зарегистрированные пользователи ИС предприятия
Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия	<ul style="list-style-type: none"> - персонал, обслуживающий технические средства; -сотрудники, задействованные в разработке и сопровождении программного обеспечения; - руководители различных уровней; - зарегистрированные пользователи ИС предприятия; представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации ; - сотрудники структурных подразделений, обеспечивающие безопасность на предприятии.

Продолжение таблицы 7

Угроза	Нарушитель
Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи	<ul style="list-style-type: none"> -сотрудники структурных подразделений, обеспечивающие безопасность на предприятии; -персонал, обслуживающий технические средства; - бывшие сотрудники предприятия; - лица, случайно или умышленно нарушившие пропускной режим; - объединенная хакерская группа.
Нарушения технологии обработки информации	<ul style="list-style-type: none"> -сотрудники структурных подразделений, обеспечивающие безопасность на предприятии; -сотрудники, задействованные в разработке и сопровождении программного обеспечения; -руководители различных уровней; -бывшие сотрудники предприятия;

7 Анализ и оценка уязвимостей активов автоматизированной системы

Были определены уязвимости активов, которые могут быть использованы источниками угроз, чтобы причинить ущерб активам системы, и, следовательно, деятельности организации. Уязвимость необходимо оценивать индивидуально и в совокупности, чтобы рассмотреть сложившуюся ситуацию в целом.

Перечень условных обозначений идентифицированных уязвимостей активов приведен в таблице 8.

Таблица 8 - Условные обозначения идентифицированных уязвимостей

Условное обозначение	Уязвимость
УЯ1	Недостаточное техническое обслуживание сервера
УЯ2	Неконтролируемое копирование информации
УЯ3	Широко известные дефекты программных средств
УЯ4	Применение прикладных программ для несоответствующих, с точки зрения времени, данных
УЯ5	Незащищенное хранение данных
УЯ6	Отсутствие «завершения сеанса» при уходе с рабочего места
УЯ7	Незащищенные линии связи
УЯ8	Плохая разводка кабелей
УЯ9	Ненадлежащее использование программных и аппаратных средств
УЯ10	Отсутствие механизмов мониторинга
УЯ11	Неправильные параметры установки программ
УЯ12	Отсутствие или неэффективное тестирование программного обеспечения

Информационными активами будут являться:

ИА1 - информация для отладки(служебные файлы);

ИА2 - общедоступная технологическая информация;

ИА3 - исходные коды ПО;

ИА4 - описание ПО;

ИА5 - протоколы;

ИА6 - интерфейсы;

ИА7 - технологическая документация.

Программно-аппаратные средства:

ПАА1 - автоматизированные рабочие места (АРМ) инженеров-программистов.

Аппаратные средства:

АА1 - сервер базы данных;

АА2 - файловый сервер;

АА3 - прокси сервер.

Возможность использования уязвимостей следующая:

– В – высокая вероятность использования уязвимостей, обусловленная высокой доступностью и частотой использования для реализации угроз;

– С – средняя вероятность использования уязвимостей, обусловленная небольшой доступностью и частотой использования для реализации угроз;

– Н – низкая вероятность использования уязвимостей, обусловленная низкой доступностью и частотой использования для реализации угроз.

Таблица 9 - Возможность использования уязвимостей

Угроза	Актив	Уязвимость	Возможность использования уязвимостей
[У1] утечка информации по техническим каналам	ИА1-7	[УЯ7] Незащищенные линии связи; [УЯ8] Плохая разводка кабелей.	С
[У2] противоправные сбор и использование информации	ИА1,3-7 ПАА1 АА1-3	УЯ[2] Неконтролируемое копирование информации; УЯ[5] Незащищенное хранение данных; УЯ[10] Отсутствие механизмов мониторинга.	С

Продолжение таблицы 9

Угроза	Актив	Уязвимость	Возможность использования уязвимостей
[У3] разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации	ИА1-3,5-7 ПАА1	УЯ[4]Применение прикладных программ для несоответствующих, с точки зрения времени, данных; УЯ[11] Неправильные параметры установки программ; УЯ[12] Отсутствие или неэффективное тестирование программного обеспечения.	В
[У4]Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия	ПАА1 АА1-3 ИА3,5,6	УЯ[1]Недостаточное техническое обслуживание сервера; УЯ[3]Широко известные дефекты программных средств; УЯ[10] Отсутствие механизмов мониторинга	С
[У5]Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи	ПАА1 АА1-3	УЯ[5]Незащищенное хранение данных	С
[У6] Нарушение технологии обработки информации	ИА1-7 ПАА1 АА1	УЯ[9]Ненадлежащее использование программных и аппаратных средств; УЯ[3]Широко известные дефекты программных средств	Н

Продолжение таблицы 9

Угроза	Актив	Уязвимость	Возможность использования уязвимостей
[У7] несанкционированный доступ к информации, находящейся в банках и базах данных	ПАА1 АА1-3	УЯ[1] Недостаточное техническое обслуживание сервера;	В
[У8] нарушение законных ограничений на распространение информации	ИА 1,3,7	Неконтролируемое копирование информации; Отсутствие «завершения сеанса» при уходе с рабочего места; Отсутствие механизмов мониторинга	С

Наибольшая возможность использования уязвимостей встретится при угрозе: разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации активов ИА1-3,5-7 ПАА1 уязвимостей: Применение прикладных программ для несоответствующих, с точки зрения времени, данных, неправильные параметры установки программ, отсутствие или неэффективное тестирование программного обеспечения.

8 Анализ рисков информационной безопасности

Анализ рисков в области ИБ может быть качественным и количественным. Количественный анализ точнее, он позволяет получить конкретные значения рисков, но он занимает больше времени. Чаще всего бывает достаточно быстрого качественного анализа, задача которого - распределение факторов риска по группам. Шкала качественного анализа может различаться в разных методах оценки, но всё сводится к тому, чтобы выявить самые серьезные угрозы. Существует несколько моделей качественного анализа. Варианты различаются лишь количеством градаций риска. Одна из самых распространенных моделей - трехступенчатая. Каждый фактор оценивается по шкале “низкий - средний - высокий”.

В предыдущих главах были проведены:

- идентификация и оценка ценности активов;
- анализ и оценка угроз информационной безопасности;
- анализ и оценка уязвимостей активов автоматизированной системы,

в которых был осуществлен качественный анализ.

Анализ рисков показал, наиболее ценными активами являются:
информация для отладки (служебные файлы);

- АРМ инженеров-программистов;
- сервер БД;
- исходные коды ПО;
- технологическая документация;
- файловый сервер

Наиболее высокая возможность реализации угроз у следующих угроз:

- утечка информации по техническим каналам;
- противоправные сбор и использование информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- нарушения технологии обработки информации;

- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

9 Оценивание рисков информационной безопасности

Оценивание риска является процессом сравнения результатов анализа риска с критериями риска с целью определения является ли риск и (или) его величина приемлемыми или допустимыми.

В качестве метода оценки рисков информационной безопасности используется метод ранжирования активов мерами рисков. Для реализации данного метода необходимо предварительно определить значения рисков ИБ в зависимости от актива, уровня реализации угроз и возможности использования уязвимости.

Уровень реализации угроз представлен ранее в таблице 5. Значения ценности активов определены в таблицах 2 и 3. Возможность использования уязвимости представлена в таблице 9.

Значение ценности актива, уровень реализации угроз и возможность использования уязвимости объединяются в матрицу, с целью определения соответствующей меры риска по выбранной шкале для каждой комбинации. Значения рисков ИБ устанавливаются экспертным путем, представлены в таблице 10.

Таблица 10 - Значения рисков ИБ

Возможность реализации угрозы	Низкий уровень реализации угрозы (Н)			Средний уровень реализации угрозы (С)			Высокий уровень реализации угрозы (В)		
Возможность использования уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение ценности актива									
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6

Продолжение таблицы 10

Возможность реализации угрозы	Низкий уровень реализации угрозы (Н)			Средний уровень реализации угрозы (С)			Высокий уровень реализации угрозы (В)		
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
5	5	6	7	6	7	8	7	8	9

Ниже приведены условные обозначения:

- У1 - утечка информации по техническим каналам;
- У2 - противоправные сбор и использование информации;
- У3 - разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- У4 - внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- У5 – уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- У6 - нарушение технологии обработки информации;
- У7 - несанкционированный доступ к информации, находящейся в банках и базах данных;
- У8 - нарушение законных ограничений на распространение информации.

Оценивание рисков ИБ активов отдела АО «ПНИЭИ» представлено в таблицах 11-21.

Таблица 11 – Оценивание рисков ИБ актива «Информация для отладки (служебные файлы)»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Информация для отладки (служебные файлы);	5	У1	В	С	8	37
		У2	В	С	8	
		У3	С	В	8	
		У6	С	Н	6	
		У8	С	С	7	

Таблица 12 – Оценивание рисков ИБ актива «Общедоступная технологическая информация»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Общедоступная технологическая информация	2	У1	В	С	5	13
		У3	С	В	5	
		У6	С	Н	3	

Таблица 13 – Оценивание рисков ИБ актива «Исходные коды ПО»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Исходные коды ПО	4	У1	В	С	7	38
		У2	В	С	7	
		У3	С	В	7	
		У4	С	С	6	

Продолжение таблицы 13

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Исходные коды ПО	4	У6	С	Н	5	38
		У8	С	С	6	

Таблица 14 – Оценивание рисков ИБ актива «Описание ПО»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использова- ния уязвимости	Значе- ние риска	Общее значени е риска
Описание ПО	3	У1	В	С	6	16
		У2	В	С	6	
		У6	С	Н	4	

Таблица 15 – Оценивание рисков ИБ актива «Протоколы»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использова- ния уязвимости	Значе- ние риска	Общее значе- ние риска
Протоколы	2	У1	В	С	5	22
		У2	В	С	5	
		У3	С	В	5	
		У4	С	С	4	
		У6	С	Н	3	

Таблица 16 - Оценивание рисков ИБ актива «Интерфейсы»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Интерфейсы	3	У1	В	С	6	27
		У2	В	С	6	
		У3	С	В	6	

Продолжение таблицы 16

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Интерфейсы	3	У4	С	С	5	27
		У6	С	Н	4	

Таблица 17 - Оценивание рисков ИБ актива «Технологическая документация»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Технологическая документация	4	У1	В	С	7	32
		У2	В	С	7	
		У3	С	В	7	
		У6	С	Н	5	
		У8	С	С	6	

Таблица 18 - Оценивание рисков ИБ актива «АРМ»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
АРМ	5	У2	В	С	8	43
		У3	С	В	8	
		У4	С	С	7	
		У5	Н	С	6	
		У6	С	Н	6	
		У7	С	В	8	

Таблица 19 - Оценивание рисков ИБ актива «Файловый сервер»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Файловый сервер	4	У2	В	С	7	25
		У4	С	С	6	
		У5	Н	С	5	
		У7	С	В	7	

Таблица 20 - Оценивание рисков ИБ актива «Сервер БД»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Сервер БД	5	У2	В	С	8	35
		У4	С	С	7	
		У5	Н	С	6	
		У6	С	Н	6	
		У7	С	В	8	

Таблица 21 - Оценивание рисков ИБ актива «Прокси сервер»

Актив	Значение ценности актива	Угроза	Возможность реализации угрозы	Возможность использования уязвимости	Значение риска	Общее значение риска
Прокси сервер	3	У2	В	С	6	21
		У4	С	С	5	
		У5	Н	С	4	
		У7	С	В	6	

Таблица 22 - Результаты ранжирования активов мерами рисков

Актив	Общее значение риска	Ранг риска
Информация для отладки (служебные файлы)	37	3
Общедоступная технологическая информация	13	11
Исходные коды ПО	38	2
Описание ПО	16	10
Протоколы	22	8
Интерфейсы	27	6
Технологическая документация	32	5
АРМ инженеров-программистов	42	1
Файловый сервер	25	7
Сервер БД	35	4
Прокси сервер	21	9

Исходя из таблицы 22, наиболее уязвимыми активами отделов по разработке ПО являются:

- АРМ инженеров - программистов;
- исходные коды ПО;
- информация для отладки (служебные файлы);
- сервер БД;
- технологическая документация;
- интерфейсы.

10 Определение способов обработки рисков информационной безопасности

Обработка рисков ИБ является процессом выбора и реализации защитных мер для снижения риска.

Различают следующие способы обработки рисков ИБ:

- предотвращение риска;
- перенос риска;
- снижение риска;
- принятие риска.

Предотвращение риска – решение не быть вовлеченным в рискованную ситуацию или действия предупреждающие влечение в ней.

Перенос риска – разделение с другой стороной потерь от риска.

Снижение риска – действие, предпринятое для уменьшения вероятности негативных последствий или их вместе, связанных с риском.

Снижение риска может осуществляться через:

- уменьшение угроз;
- уменьшение уязвимостей.

Принятие риска – проверка оцененных и обработанных рисков.

Возможно два подхода принятия риска:

- принятие риска при успешном снижении риска;
- принятие риска при сохранении риска.

На принятие риска влияют следующие факторы:

- возможные последствия осуществления риска;
- ожидаемая частота подобных событий;
- готовность к принятию риска;
- доступные финансовые, кадровые, информационные ресурсы.

Способы обработки рисков ИБ для активов приведены в таблице 23.

Таблица 23 - Способы обработки рисков ИБ для активов.

Актив	Способ обработки рисков ИБ
АРМ	Снижение риска

Продолжение таблицы 23

Актив	Способ обработки рисков ИБ
Исходные коды ПО	Снижение риска
Информация для отладки (служебные файлы)	Снижение риска
Сервер БД	Снижение риска
Технологическая документация	Снижение риска
Интерфейсы	Снижение риска
Файловый сервер	Снижение риска
Протоколы	Снижение риска
Прокси сервер	Снижение риска
Описание ПО	Снижение риска
Общедоступная технологическая информация	Принятие риска

Как видно из таблицы 23, для актива «Общедоступная технологическая информация» был выбран способ обработки рисков информационной безопасности - принятие риска, для остальных активов будет осуществлен способ – снижение риска.

11 Выбор мер по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии.

Защитные меры были выбраны для следующих областей информационной безопасности:

- управление активами;
- ИБ, связанная с персоналом;
- контроля доступа;
- управления непрерывности бизнеса.

Меры по защите информации можно разделить на 2 типа:

- организационные меры;
- технические меры.

Организационные меры включают в себя следующие действия: работу с персоналом, контроль режима защиты документов, определение формы и содержания документов.

В информационные активы включаются: исходные коды ПО, информация для отладки(служебные файлы), технологическая документация, интерфейсы, протоколы, описание ПО.

Под программно-аппаратными средствами будут пониматься АРМ инженеров-программистов.

В соответствии с ТЗ на ВКР, меры по защите конфиденциальности информации для автоматизированной системы должны осуществляться в соответствии со статьей 10 и статьей 11 Федерального закона от 29.07.2004 №98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне".

Таким образом, защитными мерами являются:

- определение перечня информации, составляющей коммерческую тайну (ЗМ1);
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка (ЗМ2);

– учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана (ЗМ3);

– регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров (ЗМ4);

– нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (ЗМ5);

– обязанность работодателя ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну (ЗМ6);

– обязанность работодателя ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение (ЗМ7);

– обязанность работодателя создать для работника необходимых условий для соблюдения им установленного работодателем режима коммерческой тайны (ЗМ8);

– обязанность работника выполнить установленные работодателем режимом коммерческой тайны (ЗМ9);

– обязанность работника не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора (ЗМ10);

- обязанность работника возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей (ЗМ11);

- обязанность работника передать работодателю при прекращении или расторжении трудового договора материальных носителей информации, имеющих в пользовании работника и содержащих информацию, составляющую коммерческую тайну (ЗМ12).

В соответствии с ТЗ на ВКР, для обеспечения защиты информации, содержащейся в информационной системе отделов предприятия по разработке программного обеспечения, должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации в соответствии со статьей 25 Федерального закона от 27.12.2002 №184-ФЗ (ред. от 28.11.2015) "О техническом регулировании".

Отсюда следует, что одной из защитных мер является применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации (ЗМ13). Также необходимо использовать следующие защитные меры:

- следует использовать средства информационной безопасности на уровне операционной системы для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать идентификацию и верификацию компьютера пользователя, терминала и местоположение каждого авторизованного пользователя; регистрацию успешных и неудавшихся доступов к системе; аутентификацию соответствующего уровня; ограничение времени подсоединения пользователей (ЗМ14).

- системы, обрабатывающие конфиденциальную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой (ЗМ15).

- пользователи должны обеспечивать соответствующую защиту АРМ, оставленного без присмотра: необходимо завершать активные сеансы по

окончанию работы, если отсутствует механизм блокировки; отключаться от мэйнфрейма, когда сеанс закончен; использовать пароль, когда АРМ не используется (ЗМ16).

– доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, включающий использование уникальных ID пользователей, проверку авторизации пользователя от владельца системы на пользование информационной системой или сервисов, проверку уровня предоставления доступа соответствия производственной необходимости, предоставление документа пользователям с указанием их прав доступа, периодическую проверку и удаление избыточных пользовательских ID и учетных записей (ЗМ17).

Защитные меры в области управления активами приведены в таблице 24. Защитные меры в области ИБ связанная с персоналом приведены в таблице 25. Защитные меры в области контроля доступа приведены в таблице 26. Защитные меры в области управления непрерывностью бизнеса приведены в таблице 27.

Таблица 24 - Защитные меры в области управления активами

Актив	Защитные меры
Информационные активы	ЗМ1, ЗМ2, ЗМ4, ЗМ5
Программно – аппаратные средства	ЗМ13,ЗМ15, ЗМ17
Файловый сервер, Сервер БД, Прокси сервер	ЗМ13,ЗМ15,ЗМ17

Таблица 25 - Защитные меры в области ИБ связанная с персоналом

Актив	Защитные меры
Информационные активы	ЗМ2 - ЗМ4, ЗМ6 – ЗМ12
Программно – аппаратные средства	ЗМ13,ЗМ14,ЗМ16
Файловый сервер, Сервер БД, Прокси сервер	ЗМ13,ЗМ14,ЗМ16

Таблица 26 - Защитные меры в области контроля доступа

Актив	Защитные меры
Информационные активы	ЗМ2 – ЗМ12
Программно – аппаратные средства	ЗМ13,ЗМ14,ЗМ15,ЗМ17
Файловый сервер, Сервер БД, Прокси сервер	ЗМ13, ЗМ14,ЗМ15,ЗМ17

Таблица 27 - Защитные меры в области управления непрерывностью бизнеса

Актив	Защитные меры
Информационные активы	ЗМ8 - ЗМ12
Программно – аппаратные средства	ЗМ13
Файловый сервер, Сервер БД, Прокси сервер	ЗМ13

ЗАКЛЮЧЕНИЕ

В процессе дипломной работы выполнены следующие задачи:

- проведен анализ проблемы защиты конфиденциальной информации;
- разработана структура автоматизированной системы отделов по разработке программного обеспечения;
- разработана модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения;
- проведена идентификация и оценка ценности активов;
- осуществлен анализ и оценка угроз информационной безопасности;
- разработана модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения;
- осуществлен анализ и оценка уязвимостей активов автоматизированной системы;
- проведен анализ рисков информационной безопасности;
- проведено оценивание рисков информационной безопасности;
- определены способы обработки рисков информационной безопасности;
- осуществлен выбор мер по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии.

В результате дипломной работы разработана методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Таким образом, цель дипломной работы достигнута, требования технического задания на выпускную квалификационную работу выполнены в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 №Пр-1895)

2 Приказ Гостехкомиссии России от 30.08.02 №282 «Специальные требования и рекомендации по технической защите конфиденциальной информации».

3 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

4 ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации. Основные термины и определения.

5 ГОСТ 34.003-90 Автоматизированные системы. Термины и определения.

6 ГОСТ Р ИСО/МЭК 13335-1-2006. Методы и средства обеспечения безопасности.

7 Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне".

8 Направления деятельности АО «ПНИЭИ» [Электронный ресурс]: сайт АО «ПНИЭИ». – 2016. – Режим доступа: <http://пниэи.рф/activity/index.htm>, свободный. – Загл. с экрана

9 Федеральный закон от 27.12.2002 №184-ФЗ (ред. от 28.11.2015) "О техническом регулировании".

ПРИЛОЖЕНИЕ А

(обязательное)

Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ»

1. Цели методики

Основными целями методики является:

- обеспечение сохранности, целостности конфиденциальной информации, используемой при разработке программного обеспечения, и предоставление доступа к ней в строгом соответствии с установленными приоритетами и правилами разграничения доступа;
- обеспечение защиты аппаратных и программно-аппаратных ресурсов от угроз информационной безопасности;
- обеспечение защиты конфиденциальной информации, используемой при разработке программного обеспечения, от угроз информационной безопасности;
- снижение угроз информационной безопасности до приемлемого для АО «ПНИЭИ» уровня.

2. Описание защищаемых активов автоматизированной системы отделов по разработке программного обеспечения

В отделах по разработке программного обеспечения (ПО) АО «ПНИЭИ» определены следующие виды защищаемых активов:

- информационные активы: информация для отладки (служебные файлы), общедоступная технологическая информация, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая документация;
- программно-аппаратные активы: автоматизированные рабочие места (АРМ) инженеров-программистов;
- аппаратные активы: сервер баз данных, файловый сервер, прокси-сервер.

Активами отдела по разработке ПО, имеющими наибольшую ценность, являются:

- исходные коды ПО;
- АРМ инженеров-программистов;
- сервер базы данных (БД).

Наибольшему риску подвержены следующие активы:

- АРМ инженеров-программистов;
- исходные коды ПО;
- информация для отладки(служебные файлы)
- сервер БД;
- технологическая документация;
- файловый сервер.

3. Описание уязвимостей активов автоматизированной системы

В АС отделов по разработке ПО могут быть обнаружены следующие уязвимости активов АС:

- недостаточное техническое обслуживание сервера;
- неконтролируемое копирование информации;
- широко известные дефекты программных средств;
- применение прикладных программ для несоответствующих, с точки зрения времени, данных;
- незащищенное хранение данных;
- отсутствие «завершения сеанса» при уходе с рабочего места;
- незащищенные линии связи;
- плохая разводка кабелей;
- ненадлежащее использование программных и аппаратных средств;
- отсутствие механизмов мониторинга;
- неправильные параметры установки программ;
- отсутствие или неэффективное тестирование программного обеспечения.

4. Описание актуальных угроз информационной безопасности для автоматизированной системы

Угрозами, актуальными для АС отделов по разработке ПО являются:

- утечка информации по техническим каналам;
- противоправные сбор и использование информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- нарушение технологии обработки информации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Организация системы защиты должна быть направлена на снижение возможностей реализации данных угроз.

5. Модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения

Первая угроза - Утечка информации по техническим каналам.

Методом нападения, которым осуществляется данная угроза, являются информационно-технические воздействия.

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи.

Объекты защиты: информация, обрабатываемая на АРМ; информация, обрабатываемая на серверах; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

- риск денежной потери - средний;
- риск потери производительности - низкий;
- риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как средний.

Источники угроз: Лица, не имеющие доступа к АСУ .

Вторая угроза - Противоправные сбор и использование информации.

Методами нападения, которыми осуществляется данная угроза, являются информационно-технические воздействия с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи; отказ технических средств и сбой программного обеспечения в информационных и телекоммуникационных системах.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

риск денежной потери - высокий;

риск потери производительности - высокий;

риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Лица, не имеющие доступа к АСУ.

Третья угроза - Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации

Методами нападения, которыми осуществляется данная угроза, являются информационно-технические воздействия с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

Данные методы используют следующие уязвимости: несовершенства средств защиты информации и систем связи.

Объекты защиты: информация, обрабатываемая на АРМ ; информация,

обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

риск денежной потери - высокий;

риск потери производительности - высокий;

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Четвертая угроза - Нарушения технологии обработки информации.

Методами нападения, которыми осуществляется данная угроза, являются несанкционированные действия с защищаемой информацией.

Данные методы используют следующие уязвимости: дефицит квалифицированных кадров.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации.

Данной угрозе присущи следующие типы потерь:

риск денежной потери - высокий;

риск потери производительности - высокий;

риск затруднения деятельности - средний.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Пятая угроза - Несанкционированный доступ к информации, находящейся в банках и базах данных.

Методом нападения, которым осуществляется данная угроза, является несанкционированный доступ к защищаемой информации.

Данный метод использует следующие уязвимости: несовершенства средств защиты информации и систем связи; отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных

системах.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

риск денежной потери - высокий;

риск потери производительности - высокий;

риск затруднения деятельности - средний.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации.

Шестая угроза - Нарушение законных ограничений на распространение информации.

Методами нападения, которыми осуществляется данная угроза, являются несанкционированные действия с защищаемой информацией.

Данный метод использует следующие уязвимости: несовершенства средств защиты информации и систем связи; дефицит квалифицированных кадров.

Объекты защиты: информация, обрабатываемая на АРМ ; информация, обрабатываемая на серверах АСУ ; информация, содержащаяся на электронном или бумажном носителе информации; информация, передаваемая через подсистемы передачи информации.

Данной угрозе присущи следующие типы потерь:

риск денежной потери - высокий;

риск потери производительности - высокий;

риск затруднения деятельности - высокий.

Масштаб ущерба характеризуется как высокий.

Источники угроз: Персонал, имеющий доступ к защищаемой информации.

Модель нарушителя ИБ

Всех потенциальных нарушителей можно подразделить на:

- внешних нарушителей, осуществляющих атаки из за пределов контролируемой зоны;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

Внутренние нарушители:

В качестве потенциальных внутренних нарушителей АО «ПНИЭИ» рассматриваются:

- зарегистрированные пользователи ИС предприятия;
- сотрудники предприятия, являющиеся сотрудниками, не допущенные к информационным ресурсам, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства;
- сотрудники структурных подразделений, обеспечивающие безопасность на предприятии;
- сотрудники, задействованные в разработке и сопровождении программного обеспечения;
- руководители различных уровней.

Внешние нарушители.

В качестве потенциальных внешних нарушителей АО «ПНИЭИ» рассматриваются:

- бывшие сотрудники предприятия;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго- , водо-, теплоснабжения и т.п.);
- посетители (приглашенные по какому либо поводу);
- лица, случайно или умышленно нарушившие пропускной режим;
- конкурирующие с предприятием организации;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

— лица, случайно или умышленно проникшие в ИС из внешней сети (хакеры).

Цели, преследуемые нарушителями, могут быть следующие:

- сбор информации;
- финансовая выгода;
- конкурентная выгода;
- месть;
- любопытство.

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

- нарушитель скрывает свои действия от других сотрудников;
- внутренний и внешний нарушитель могут быть в сговоре;
- в своей деятельности нарушитель может использовать любое средство для перехвата информации, воздействия на информацию и другие средства для достижения поставленных перед ним целей

6. Описание рисков информационной безопасности автоматизированной системы

Способом обработки рисков информационных активов (информация для отладки, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая документация) является снижение риска.

Способом обработки актива общедоступная технологическая информация является принятие риска.

Способом обработки рисков программно-аппаратных активов (АРМ инженеров-программистов) является снижение риска.

Способом обработки рисков сервера БД, файлового сервера, прокси-сервера является снижение риска.

Реализация актуальных угроз ИБ для АС отделов по разработке ПО АО «ПНИЭИ» наносит ущерб организации и приводит к следующим последствиям:

- прерывание основной деятельности организации;
- финансовые и материальные затраты.

7. Перечень защитных мер по защите конфиденциальной информации для автоматизированной системы

Для снижения рисков ИБ должны быть реализованы защитные меры.

Для информационных активов (информация для отладки, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая документация) в области управления активами выделены следующие защитные меры:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации.

Для программно-аппаратных активов (АРМ инженеров-программистов) в области управления активами выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации;
- системы, обрабатывающие конфиденциальную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой;
- доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, включающий использование уникальных ID пользователей,

проверку авторизации пользователя от владельца системы на пользование информационной системой или сервисов, проверку уровня предоставления доступа соответствия производственной необходимости, предоставление документа пользователям с указанием их прав доступа, периодическую проверку и удаление избыточных пользовательских ID и учетных записей.

Для активов (сервер БД, файловый сервер, прокси-сервер) в области управления активами выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации;
- системы, обрабатывающие конфиденциальную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой;
- доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, включающий использование уникальных ID пользователей, проверку авторизации пользователя от владельца системы на пользование информационной системой или сервисов, проверку уровня предоставления доступа соответствия производственной необходимости, предоставление документа пользователям с указанием их прав доступа, периодическую проверку и удаление избыточных пользовательских ID и учетных записей.

Для информационных активов (информация для отладки, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая документация) в области ИБ, связанной с персоналом, выделены следующие защитные меры:

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

– регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

– обязанность работодателя ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

– обязанность работодателя ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

– обязанность работодателя создать для работника необходимых условий для соблюдения им установленного работодателем режима коммерческой тайны;

– обязанность работника выполнить установленные работодателем режимом коммерческой тайны;

– обязанность работника не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

– обязанность работника возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

– обязанность работника передать работодателю при прекращении или расторжении трудового договора материальных носителей информации, имеющих в пользовании работника и содержащих информацию, составляющую коммерческую тайну.

Для программно-аппаратных активов (АРМ инженеров-программистов) в области ИБ, связанной с персоналом, выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации

- следует использовать средства информационной безопасности на уровне операционной системы для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать идентификацию и верификацию компьютера пользователя, терминала и местоположение каждого авторизованного пользователя; регистрацию успешных и неудавшихся доступов к системе; аутентификацию соответствующего уровня; ограничение времени подсоединения пользователей;

- пользователи должны обеспечивать соответствующую защиту АРМ, оставленного без присмотра: необходимо завершать активные сеансы по окончании работы, если отсутствует механизм блокировки; отключаться от мейнфрейма, когда сеанс закончен; использовать пароль, когда АРМ не используется.

Для активов (сервер БД, файловый сервер, прокси-сервер) в области ИБ, связанной с персоналом, выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации;

- следует использовать средства информационной безопасности на уровне операционной системы для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать идентификацию и верификацию компьютера пользователя, терминала и местоположение каждого авторизованного пользователя; регистрацию успешных и неудавшихся доступов к системе; аутентификацию соответствующего уровня; ограничение времени подсоединения пользователей;

- пользователи должны обеспечивать соответствующую защиту АРМ, оставленного без присмотра: необходимо завершать активные сеансы по окончании работы, если отсутствует механизм блокировки; отключаться от

мэйнфрейма, когда сеанс закончен; использовать пароль, когда АРМ не используется.

Для информационных активов (информация для отладки, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая документация) в области контроля доступа выделены следующие защитные меры:

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка ;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана ;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации;

- обязанность работодателя ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

- обязанность работодателя ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

- обязанность работодателя создать для работника необходимых условий для соблюдения им установленного работодателем режима коммерческой тайны;

- обязанность работника выполнить установленные работодателем режимом коммерческой тайны;

- обязанность работника не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

- обязанность работника возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

- обязанность работника передать работодателю при прекращении или расторжении трудового договора материальных носителей информации, имеющих в пользовании работника и содержащих информацию, составляющую коммерческую тайну.

Для программно-аппаратных активов (АРМ инженеров-программистов) в области контроля доступа выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации;

- следует использовать средства информационной безопасности на уровне операционной системы для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать идентификацию и верификацию компьютера пользователя, терминала и местоположение каждого авторизованного пользователя; регистрацию успешных и неудавшихся доступов к системе; аутентификацию соответствующего уровня; ограничение времени подсоединения пользователей;

- системы, обрабатывающие конфиденциальную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой;

- доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации

пользователей, включающий использование уникальных ID пользователей, проверку авторизации пользователя от владельца системы на пользование информационной системой или сервисов, проверку уровня предоставления доступа соответствия производственной необходимости, предоставление документа пользователям с указанием их прав доступа, периодическую проверку и удаление избыточных пользовательских ID и учетных записей.

Для активов (сервер БД, файловый сервер, прокси-сервер) в области контроля доступа выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации;

- следует использовать средства информационной безопасности на уровне операционной системы для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать идентификацию и верификацию компьютера пользователя, терминала и местоположение каждого авторизованного пользователя; регистрацию успешных и неудавшихся доступов к системе; аутентификацию соответствующего уровня; ограничение времени подсоединения пользователей;

- системы, обрабатывающие конфиденциальную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой;

- доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, включающий использование уникальных ID пользователей, проверку авторизации пользователя от владельца системы на пользование информационной системой или сервисов, проверку уровня предоставления доступа соответствия производственной необходимости, предоставление документа пользователям с указанием их прав доступа, периодическую проверку и удаление избыточных пользовательских ID и учетных записей.

Для информационных активов (информация для отладки, исходные коды ПО, описание ПО, протоколы, интерфейсы, технологическая

документация) в области управления непрерывностью бизнеса выделены следующие защитные меры:

- обязанность работодателя создать для работника необходимых условий для соблюдения им установленного работодателем режима коммерческой тайны;

- обязанность работника выполнить установленные работодателем режимом коммерческой тайны;

- обязанность работника не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

- обязанность работника возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

- обязанность работника передать работодателю при прекращении или расторжении трудового договора материальных носителей информации, имеющих в пользовании работника и содержащих информацию, составляющую коммерческую тайну.

Для программно-аппаратных активов (АРМ инженеров-программистов) в области управления непрерывностью бизнеса выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации.

Для активов (сервер БД, файловый сервер, прокси-сервер) в области ИБ, связанной с персоналом, выделены следующие защитные меры:

- применение средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации.

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа 11ПИ1

УТВЕРЖДАЮ
Зав. кафедрой ИБСТ
к.т.н., ~~доцент~~ С.Л. Зефиров
«27» 04 2016 г.

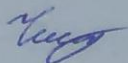
**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ
РАБОТУ**

студента группы 11ПИ1 Борисова Андрея Евгеньевича

Специальность 100503 – Информационная безопасность
автоматизированных систем

Тема дипломной работы: Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Руководитель ВКР
инженер АО «ПНИЭИ»

 Чистова Мария Сергеевна

Нормоконтролер
к.т.н., доцент



Иванов А.П.

1 Цели и задачи ВКР

Цель работы: разработка методики защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Разрабатываемая методика предназначена для использования в отделах предприятия АО «ПНИЭИ» по разработке программного обеспечения.

2 Тактико-технические требования к выполнению ВКР

Технические требования:

- в результате выпускной квалификационной работы должен быть разработан документ "Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ» (далее – методика);
- разрабатываемая методика должна содержать:
 - цели методики;
 - описание защищаемых активов автоматизированной системы отделов по разработке программного обеспечения (далее - автоматизированной системы);
 - описание уязвимостей активов автоматизированной системы;
 - описание актуальных угроз информационной безопасности для автоматизированной системы;
 - модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения;
 - описание рисков информационной безопасности автоматизированной системы;
 - перечень защитных мер по защите конфиденциальной информации для автоматизированной системы;

– при разработке методики необходимо руководствоваться следующими требованиями и законодательными нормативными документами:

– перечень угроз информационной безопасности для автоматизированной системы должен быть составлен согласно документу "Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 №Пр-1895);

– меры по защите конфиденциальности информации для автоматизированной системы должны осуществляться в соответствии со статьей 10 и статьей 11 Федерального закона от 29.07.2004 №98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне";

– для обеспечения защиты информации, содержащейся в информационной системе отделов предприятия по разработке программного обеспечения, должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации в соответствии со статьей 5 Федерального закона от 27.12.2002 №184-ФЗ (ред. от 28.11.2015) "О техническом регулировании".

В ВКР должны быть рассмотрены следующие вопросы:

- анализ проблемы защиты конфиденциальной информации;
- структура автоматизированной системы отделов по разработке программного обеспечения;
- модель информационных потоков автоматизированной системы отделов по разработке программного обеспечения;
- идентификация и оценка ценности активов;
- анализ и оценка угроз информационной безопасности;
- модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения;
- анализ и оценка уязвимостей активов автоматизированной системы;
- анализ рисков информационной безопасности;
- оценивание рисков информационной безопасности;

- определение способов обработки рисков информационной безопасности;
- выбор мер по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

структура взаимодействия отделов по разработке программного обеспечения - 1л., ф. А1 (плакат);

модель информационных потоков взаимодействия отделов по разработке программного обеспечения - 1л., ф. А1 (плакат);

перечень уязвимостей и актуальных угроз информационной безопасности предприятия – 1л., ф. А1 (плакат);

модель угроз и модель нарушителя безопасности конфиденциальной информации при разработке программного обеспечения – 1л., ф. А1 (плакат);

меры по защите конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии – 2л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

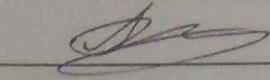
4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № 491/40 от «15» 04 2016 г.

Дата выдачи задания «15» февраля 2016 г.

Время дипломного проектирования с 10.04 2016 г. по 10.06 2016 г.

Задание к исполнению принял «15» января 2016 г.

Исполнитель ВКР  Борисов А.Е.



Ректору Пензенского
государственного университета
А. Д. Гулякову
студента 5 курса ФПИТЭ
очной формы обучения
Борисова Андрея Евгеньевича

заявление.

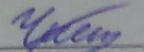
Я, Борисов Андрей Евгеньевич, студент 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломной работы на тему «Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /А.Е. Борисов/

ВКР представлена на проверку _____.

Руководитель ВКР  /М.С. Чистова/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ» студента 5 курса А.Е. Борисова специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР инженер 2 категории АО «ПНИЭИ» Чистова Мария Сергеевна.

Отчет о проверке № 1

ФИО: Иванов Алексей Петрович
дата загрузки: 03.06.2016 00:06:12
пользователь: ap_ivanov@mail.ru / ID: 1267386
отчет предоставлен сервисом «Антиплагиат»
на сайте <http://www.antiplagiat.ru>

Информация о документе

№ документа: 36
Имя исходного файла: ВКР_Борисов_АЕ_11ПНИ.doc
Размер текста: 930 кб
Тип документа: не указано
Символов в тексте: 97972
Слов в тексте: 11066
Число предложений: 340

Информация об отчете

Дата: Отчет от 03.06.2016 00:06:17 - Последний готовый отчет
Комментарий: не указано
Оценка оригинальности: 71.27%
Заимствования: 28.73%
Цитирование: 0%



Оригинальность: 71.27%
Заимствования: 28.73%
Цитирование: 0%

08.06.2016 г.

Секретарь ГЭК

М.С.Чистова

А.П.Иванов

ОТЗЫВ

на выпускную квалификационную работу студента

Пензенского государственного университета

Борисова Андрея Евгеньевича

Тема работы: Методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ»

Целью квалификационной работы Борисова А.Е. является разработка методики защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ»

Во время выполнения работы Борисовым А.Е. был изучен большой объем теоретического и практического материала, были изучены нормативные документы, связанные с оценкой и анализом рисков информационной безопасности. Изучение деятельности отделов позволило определить информационные активы, угрозы и уязвимости для информационной системы, в которой разрабатывается программное обеспечение. На основе идентифицированных угроз и уязвимостей были разработаны модель угроз и модель нарушителя, также осуществлен выбор мер по защите конфиденциальной информации. В результате дипломной работы разработана методика защиты конфиденциальной информации при разработке программного обеспечения в ходе проведения научно-исследовательских и опытно-конструкторских работ на предприятии АО «ПНИЭИ».

Следует признать, что такая работа требует большой работоспособности, терпения и упорства, которые Борисов А.Е. проявил в полной мере. Ранее дипломник зарекомендовал как ответственный специалист, соблюдающий все сроки и требования, предъявленные к данной ему работе.

Работы по всем пунктам технического задания выполнены полностью. Пояснительная записка и плакаты содержат необходимые сведения о проделанной работе.

Считаю, что дипломный проект выполнен в полном соответствии с заданием и заслуживает оценки «отлично», а дипломник Борисов Андрей Евгеньевич достоин присвоения квалификации специалиста по информационной безопасности по специальности 10.05.03 – «информационная безопасности автоматизированных систем».

Руководитель ВКР,
инженер



Чистова

/М.С. Чистова/

10.06.16

16 Баллов

РЕЦЕНЗИЯ

На выпускную квалификационную работу (далее ВКР) Борисова А.Е. на тему
МЕТОДИКА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ
РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ХОДЕ ПРОВЕДЕНИЯ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ОПЫТНО-КОНСТРУКТОРСКИХ
РАБОТ НА ПРЕДПРИЯТИИ АО «ПНИЭИ».

Достоинства ВКР:

- Результаты ВКР соответствуют её целям.
- Данная ВКР достаточно трудоёмка.
- Данная ВКР актуальна.

Недостатки ВКР:

– Не указано, что данная методика может быть использована только при разработке АО «ПНИЭИ» программного обеспечения по собственной инициативе (заказчиком является АО «ПНИЭИ»), так как в случае наличия заказчика требования к защите информации предъявляются им и регулируются существующими НМД ФСТЭК России в части государственной и/или служебной тайны;

– отсутствует анализ уже существующих методик информативно-методической литературы на исследуемую тематику;

– не указано отличие данной методики и её подхода от аналогичных (её достоинства и недостатки).

Вывод:

ВКР может быть допущена к защите в ГАК.

16.06.2016

К.Е. Логинов

9 (девятое) Баллов

