МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01спец.
_____ Титомир М.Д.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области информационных технологий и отдела информационной безопасности предприятия.

- Написание отчета по практике о проделанной работе. Проведение исследования в области информационных технологий и отдела информационной безопасности предприятия.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с задачами, функциями, правами отдела информационной безопасности предприятия.
2. Теоретически ознакомиться с организационной структурой отдела информационной безопасности предприятия и изучить экономическую эффективность системы.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Отдел информационной безопасности предприятия

Enterprise Information Security Department

Актуальность

В наше время трудно кого-либо удивить происшествиями в области информационной безопасности. Все чаще мы сталкиваемся с различными угрозами в этой области. Практически каждый день приносит все новые и новые сведения об атаках хакеров (заметим, только что обнаруженных и нередко успешных), вирусных эпидемиях, атаках со стороны обиженных сотрудников. Именно последние становятся наибольшей угрозой в различных организациях. Если вовремя не устранить угрозу, это может привести к необратимым последствиям, например кража конфиденциальной информации, паролей. Хотя необходимость создания этого отдела очевидна, многие организации пренебрегают этим, некоторые возлагают ответственность по обеспечению информационной безопасности на системного администратора, другие закупают дорогостоящее программное обеспечение. Картина вырисовывается безрадостная, а выход состоит в создании хорошо подготовленного подразделения — службы защиты информации

Следует отметить, что информационная безопасность – это комплекс организационно-технических мер, и одних лишь технических методов решения здесь недостаточно.

В данной работе будут описана организационная структура, основные функции и эффективность отдела информационной безопасности.

Общие положения

1. Отдел по защите информации, являясь самостоятельным структурным подразделением предприятия, создается и ликвидируется приказом [наименование должности руководителя предприятия].

2. Отдел непосредственно подчиняется [наименование должности руководителя предприятия].

3. Отдел возглавляет начальник, назначаемый на должность приказом [наименование должности руководителя предприятия].

4. В своей деятельности отдел руководствуется: - законодательством Российской Федерации; - уставом предприятия.

Факторы, указывающие на необходимость создания отдела

1. На предприятии создана локальная сеть.

2.На предприятии больше 10 компьютеров, которые распределены по различным помещениям.

3.На предприятии хранится или обрабатывается информация, которая не подлежит распространению и которая имеет ценность.

4.На предприятии один из компьютеров соединен с внешней сетью Интернет.

Создание отдела

Для того, чтобы разработать рациональную структуру службы информационной безопасности на предприятии, достаточную по составу и

оснащению средствами управления безопасностью, необходимо тщательно проанализировать избранную политику безопасности, соотнести вероятные угрозы и потери в случае их реализации с эффективностью системы защиты информации и финансовыми затратами на их реализацию. Только после этого руководство предприятия сможет обоснованно принять решение на создание соответствующей службы информационной безопасности

Организационная структура отдела информационной безопасности предприятия

Организационная структура предприятия должна включать в себя сепарированный от других отделений департамент информационной безопасности, который прямо подчиняется руководству, либо может быть частью службы безопасности предприятия. Он должен быть отдельным для минимизации рисков утечки информации (основным здесь является человеческий фактор и его воздействие), а также для удобства общения напрямую с руководством фирмы

Подразделения департамента информационной безопасности предприятия:

1. отдел нормативной документации по обеспечению рабочих процессов, который занимается нормативно-правовой базой и документацией по обеспечению ИБ на предприятии, может включать в себя также юристов;

2. отдел администрирования рабочими процессами, в который входят специалисты по управлению ИБ;

3. отдел внутреннего аудита информационной безопасности;

4. отдел внедрения систем защиты информации и информационных систем включает в себя специалистов с непосредственным опытом работы в сфере ИБ, а также по внедрению и эксплуатации информационных систем.

Существует несколько вариантов штатного расписания такой службы.

Например:

1. Заместитель директора по безопасности и защите информации;

2. Администратор безопасности АС - штатный сотрудник отдела защиты информации;

3. Администратор системы - штатный сотрудник отдела автоматизации;

4. Администраторы групп - штатные сотрудники подразделений, эксплуатирующих АС;

5. Менеджеры безопасности;

6. Операторы

Обязательства и методы защиты службы информационной безопасности предприятия:

1. Все действия сотрудников службы информационной безопасности организована в строгом соответствии с законами государства.

2. Все кандидаты которые хотят устроится на работу предприятия, должны проходить проверку службой ИБ. Также при увольнении сотрудники должны провести диалог с представителями службы ИБ. Все сотрудники должны проходить периодические семинары по информационной безопасности.

3. Нужно проводить анализ психологической и моральной обстановки на предприятии. Проводить учет нарушений безопасности конкретными сотрудниками. Постоянно мониторинг активность сотрудников.

4. Все данные должны быть расклассифицированы, будь то данные объектов сотрудников или ИС. У каждого субъекта должна быть своя роль в ИС. Также должна быть универсальная и защищенная система доступа субъектов к объектам информационной системы.

5. Должно быть обеспечено нормативное пространство. Для всех сотрудников должны быть процедуры, правила и методики действия на роботе. Изменения в работе правил сотрудников должны отображаться в определенных документах.

6. Варианты аутентификации сотрудников должны быть под контролем службы ИБ. Они проводят периодических осмотр слабых паролей, факты передачи паролей и т.д.

7. Регистрационные журналы ведутся по всем информационным системам. Также автоматический и выборочный ручной анализ. Все регистрационные журналы сохраняются вместе с архивами БД и резервными копиями.

8. На каждый ПК в сети должен быть установлен антивирусный набор.

9. Также должен быть учет единиц аппаратного обеспечения или их составляющих. А также установленных программ на ПК.

10. Нужно следить за новинками в сфере ИТ. Новые атаки, новые механизмы информационной безопасности, а также отзывы компетентных лиц.

11. Все линии обмена данным в ИС должны быть криптографически защищены. Любой обмен данными регистрируется в электронных журналах и снабжен средством контроля целостности.

Задачи

К задачам службы безопасности предприятия относятся:

определение перечня сведений, составляющих коммерческую тайну, а также круга лиц, которые в силу занимаемого служебного положения на предприятии имеют к ним доступ;

определение участков сосредоточения сведений, составляющих коммерческую тайну; технологического оборудования, выход из строя которого (в том числе уязвимого в аварийном отношении) может привести к большим экономическим потерям;

формирование требований к системе защиты в процессе создания и участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

планирование, организация и обеспечение функционирования системы защиты информации;

распределение между пользователями необходимых реквизитов защиты, включая установку (периодическую смену) паролей, управление средствами защиты коммуникаций и криптозащиту предаваемых, хранимых и обрабатываемых данных

координация действий с аудиторской службой, совместное проведение аудиторских проверок, контроль функционирования системы защиты и ее элементов, тестирование системы защиты;

организация обучения сотрудников СИБ в соответствии с их функциональными обязанностями; обучение пользователей АС правилам безопасной обработки информации;

определение круга предприятий, связанных с данным кооперативными связями, на которых возможен выход из-под контроля сведений, составляющих коммерческую тайну предприятия; выявление лиц на предприятии и предприятий (в том числе иностранных), заинтересованных в овладении коммерческой тайной.

расследование происшедших нарушений защиты, принятие мер реагирования на попытки НСД к информации и нарушениям правил функционирования системы защиты;

выполнение восстановительных процедур после фактов нарушения безопасности;

изучение, анализ, оценка состояния и разработка предложений по совершенствованию системы обеспечения информационной безопасности предприятия; внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения информационной безопасности.

совместная работа с представителями других организаций по вопросам безопасности - непосредственный контакт или консультации с партнерами или клиентами;

постоянная проверка соответствия принятых в организации правил безопасной обработки информации существующим правовым нормам, контроль за соблюдением этого соответствия.

Права

Отдел по защите информации имеет право:

1. Осуществлять контроль за деятельностью подразделений предприятия по выполнению ими требований информационной безопасности.

2. Давать подразделениям предприятия и отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию отдела.

3. Запрашивать и получать от всех подразделений предприятия сведения, справочные и другие материалы, необходимые для осуществления деятельности отдела.

4. Вести самостоятельную переписку с государственными и муниципальными органами по правовым вопросам.

5. Представлять в установленном порядке предприятие в органах государственной власти, иных учреждениях и организациях по вопросам, входящим в компетенцию отдела.

6. Принимать необходимые меры при обнаружении несанкционированного доступа к информации, как внутри предприятия, так извне, и докладывать о принятых мерах руководителю предприятия с представлением информации о субъектах, нарушивших режим доступа.

7. По согласованию с руководителем предприятия или заместителем директора предприятия по коммерческим вопросам привлекать экспертов и специалистов в сфере защиты информации для консультаций, подготовки заключений, рекомендаций и предложений.

Экономическая эффективность системы информационной безопасности промышленных предприятий

Сегодня на отечественных промышленных предприятиях с повышенными требованиями в области информационной безопасности затраты на обеспечение режима информационной безопасности составляют до 30% всех затрат на информационную систему, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения информационной безопасности. Даже в тех информационных системах, уровень информационной безопасности которых явно не достаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством затрат на повышение этого уровня.

Современные предприятия вынуждены функционировать в условиях динамично изменяющихся экономических, технологических, социальных, технических и других факторов. В этих условиях перед

руководством стоит задача повышения эффективности функционирования, а также обеспечения стабильности положения предприятия на рынке. Решение этой задачи во многом зависит от умения защищать, в том числе и информационную систему предприятия.

Экономические показатели эффективности являются самыми вескими при выборе варианта системы информационной безопасности. Кроме того, каждый проект при разработке и внедрении системы информационной безопасности должен завершаться проведением экспертизы и соответствующими экономическими расчетами.

Во многих отношениях затраты на создание системы информационной безопасности сходны с инвестициями, поскольку они связаны с вложением средств, риском и получением прибыли.

Существенным отличием является то, что под прибылью в данном случае следует понимать не конкретный поток финансовых ресурсов, а возможное уменьшение потерь от действия дестабилизирующих факторов.

Рассматривая потери информационной системы, необходимо отметить, что они могут быть экономическими, техническими, организационными, технологическими, причем они вытекают друг из друга, и потери на одном уровне влекут за собой потери на следующих уровнях.

Потери информационной системы — это потеря свойств информации, вычислительных, информационных ресурсов информационной системы, финансовых и прочих активов, а также потеря имиджа информационной системы и доверия между партнерами вследствие реализации угроз.

При определении данной величины следует принимать во внимание только ресурсы информационной системы, на которые могут быть покушения или которые могут быть утеряны полностью или частично. Также

следует принимать во внимание возможность восстанавливаемости ресурса в исходное состояние. Рассмотрим это с точки зрения основных принципов безопасности: конфиденциальности, целостности и доступности.

Необходимый уровень целостности и доступности восстанавливается посредством использования специальных методов и средств (то есть за счет дополнительных затрат). Следует отметить, что первоначальный уровень конфиденциальности практически не восстанавливается. Однако, если в случае нарушения конфиденциальности потерянная стоимость остается на уровне потерянных активов, то в случае нарушения целостности или доступности данный уровень увеличивается за счет привлечения дополнительных средств (ресурсов), которые призваны восстановить первоначальное состояние информационной системы.

В качестве разновидности компьютерных преступлений следует рассматривать кражу информационных ресурсов и услуг. Если их можно восстановить (то есть установить виновника и получить соответствующую компенсацию), величина потерь равна затратам на восстановление. В случае, когда это не удается, величина потерь равна стоимости похищенных ресурсов и услуг.

При исследовании потерь информационной системы следует выделить следующие разновидности:

— совокупные потенциальные потери без использования систем информационной безопасности, которые определяются ценностью активов информационных систем;

— возможные реальные потери при использовании систем информационной безопасности. Данный тип потерь является расчетным.

В то же время, при разработке эффективной системы информационной безопасности должна учитываться величина выигрыша

нарушителя, и основной задачей является сведение данной величины к минимуму.

При исследовании возможных потерь требуется изучить множество ресурсов информационной системы и потенциальных угроз и по отношению к каждому ресурсу найти комплекс решений, связанных со следующими обстоятельствами:

— определение круга заинтересованных лиц в использовании активов информационной системы;

— определение целей нарушителя;

— установление размеров выгоды, полученной нарушителем вследствие реализации одной или комплекса угроз;

— оценка размеров затрат, которые нарушитель готов понести для достижения поставленной цели.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с нормативной базой отдела информационной безопасности, ее задачами, правами, структурой и его экономической эффективностью.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. Алешников С.И. Проблемы информационной безопасности организации (предприятия) и пути их решения / Алешников С.И., Дёмин С.А., Фёдоров С.Б. // Вестник Балтийского федерального университета им. И.Канта — 2013.— Вып. 10. — с.147-154.

2. Организационная структура и персонал департамента информационной безопасности. Национальный открытый университет «Интуит» [Электронный ресурс]. URL: https://intuit.ru/studies/courses/563/419/lecture/9580?page=2

3. Балановская А.В. Экономическая эффективность системы информационной безопасности промышленных предприятий // Вестник Самарского государственного университета. 2015. № 5 (127). С. 14–20