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. С8118-10.05.01-1Спец
_____ Чистяков Н.А.
(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 информационной безопасности при удаленной работе.
- Написание отчета по практике о проделанной работе.

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 понятием информационной безопасности при удаленной работе.

2.Теоретически ознакомиться с методами предотвращения инцидентов информационной безопасности и утечек данных.

3.На основе полученных знаний написать отчет по практике о проделанной работе.

Предупреждение инцидентов информационной безопасности при удаленной работе. Предотвращение утечек данных.

Аннотация:

Проблема разглашения конфиденциальных данных является одной из значимых из-за высокой ценности информации как ресурса в наше время. В данной работе рассматриваются вопросы предупреждения инцидентов, связанных с защитой данных, рекомендации по повышению информационной безопасности предприятия в условиях дистанционной работы. Отдельно затронем предотвращение утечек конфиденциальных данных с помощью DLP-систем.

Ключевые слова: информационная безопасность, DLP-система, утечки данных, инциденты информационной безопасности.

Введение:

Для любой компании одним из важнейших приоритетов является обеспечение защиты конфиденциальной информации, составляющей коммерческую тайну. При переходе на дистанционную работу риск инцидентов и утечек ценной информации значительно возрастают по сравнению с работой в локальной, изолированной и защищенной сети предприятия, так как информация будет пересылаться по каналам связи, которые могут быть небезопасны, домашние устройства сотрудников менее защищены от атак и данные могут попасть к злоумышленникам из-за халатности работников. Особенно актуален этот вопрос сейчас, потому что многие компании массово перевели своих сотрудников на удаленную работу из дома в связи с пандемией COVID-19.

Общие способы и рекомендации для повышения информационной безопасности:

Самыми распространенными способами защиты информации, циркулирующей на предприятии являются идентификация, аутентификация и авторизация сотрудников. Аутентификация выполняется следующим образом: пользователь однократно передает эталонный образец аутентификационной информации (например, пароль) модулю аутентификации на хранение. Затем при каждой аутентификации у пользователя будет запрашиваться аутентификационная информация, которая сравнивается с эталоном. Если есть совпадение, то пользователь подлинный.

Однако, в случае удаленной аутентификации существует проблема передачи пароля по каналам связи, которые могут быть не безопасны. Для сохранности информации при пересылке используются множество протоколов аутентификации.

Другой распространенный способ защиты данных - это система криптографической защиты информации(СКЗИ). Она обеспечивает конфиденциальность, целостность, аутентификацию и невозможность отказа от авторства и широко применяется в компаниях и организациях.

В условиях дистанционной работы к СКЗИ выдвигаются следующие требования:

-криптографическое средство должно штатно функционировать совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к нему требований;

-для обеспечения безопасности персональных данных при их обработке должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства.

Рекомендации для повышения информационной безопасности:

1. Работать с облачными сервисами с улучшенными процессами идентификации (например, отправка кода авторизации посредством SMS-сообщений).

2. Использовать передачу данных в зашифрованном виде.

3. Использовать лицензионное программное обеспечение, в котором не предустановлены вирусные программы.

4. Своевременно обновлять операционную систему, приложения, драйвера,

программы до последних версий.

5. Не использовать чужие накопители данных, так как на них могут содержаться компьютерные вирусы.

6. Применять антивирусные программные продукты и сетевые экраны.

7. Работать с конфиденциальными данными на устройствах, отключенных от сети Интернет, если это возможно.

8. Использовать пароли для входа в рабочие устройства,

что позволит снизить риск утечки данных при потере устройства.

9. Систематически менять пароли от почтовых ящиков и любых других учетных записей, в которых осуществляется работа с данными или их передача.

10. В сервисах связи сотрудников (Skype,MS Teams,Zoom и т.п.)должно быть реализовано сквозное шифрование, при котором медиа-файлы и сообщения не смогут попасть в руки злоумышленника.

11. Сервисы должны позволять организаторам конференций ограничивать доступ к конференциям и допускать только тех, кто приглашен.

12. Сервисы должны позволять пользователям безопасно удалять данные из сервиса, а также полностью удалять учетные записи, которые больше не используются.

13. Использование SIEM-систем(управление информацией и событиями безопасности) позволит отслеживать действия пользователей внутри сети.

Предотвращение утечек данных.DLP-системы.

В настоящее время современной системой защиты информации коммерческих предприятий при переводе сотрудников на удаленную работу является DLP-системы в корпоративную сеть.DLP-система (от англ. Data Leak Prevention)-это программный продукт для предотвращения утечек конфиденциальной информации за пределы корпоративной сети. Для устранения утечек и вредоносной инсайдерской активности реализован перехват максимально возможного количества каналов коммуникации.

Основными каналами утечки информации являются:

─ съемные носители: USB – флеш – накопители, CD/DVD диски, съемные, жесткие диски и пр.;

─ электронная почта, в том числе личная;

─ распечатанные с компьютера документы;

─ социальные сети, сервисы для видео- и аудиозвонков и др.

DLP - системы основываются на анализе потоков данных, которые пересекают границы защищаемой информационной системы. При обнаружении в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения блокируется.

Основные функции DLP-систем:

─ контроль передачи информации через Интернет (E-Mail, HTTP, HTTPS, FTP др.);

─ контроль сохранения информации на внешние носители;

─ защита информации от утечки в печатном виде;

─ блокирование попыток пересылки/сохранения конфиденциальных данных;

─ информирование администраторов ИБ об инцидентах;

─ создание теневых копий;

─ поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов и другим признакам;

─ предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычный состав DLP-системы включает:

-центр управления и мониторинга;

-модули сетевого уровня-осуществляют контроль трафика, который пересекает периметра информационной системы. Обычно расположены на прокси-серверах, серверах электронной почты. Могут быть реализованы в виде отдельных серверов;

-компоненты уровня хоста-располагаются на рабочих станциях персонала. Контролируют запись на компакт-диски, USB-устройства и др. Компоненты уровня хоста также стараются отслеживать различные методы для обхода контроля (например, изменение сетевых настроек).

Существует 2 способа распознавания конфиденциальной информации:

-анализ формальных признаков (хэш-значения, специальные метки и т.д.)-этот способ позволяет избежать ложных срабатываний, однако требует предварительной классификации документов. Но если конфиденциальный документ не был подвержен предварительной классификации, то есть вероятность пропуска конфиденциальной информации за пределы системы.

-анализ контента-может давать ложные срабатывания, однако позволяет выявлять пересылку конфиденциальной информации не только среди документов, предварительно классифицированных.

В современных DLP-системах сочетают использование обоих видов анализа для наибольшей эффективности.

Кроме основной задачи перед DLP – системой могут стоять следующие вторичные задачи:

- архивирование пересылаемых данных, которые могут быть полезны при расследовании инцидентов информационной безопасности;

-предотвращение возможности передачи вовне не только конфиденциальной, но и другой нежелательной информации (например, спам);

-предотвращение возможности передачи нежелательной информации не только изнутри информационной системы наружу, но и снаружи внутрь информационной системы;

-предотвращение использования работниками фирменных информационных ресурсов в личных целях;

-оптимизация загрузки каналов, экономия трафика;

-контроль присутствия работников на рабочем месте;

-отслеживание надёжности сотрудников.

На данный момент существуют различные отечественные DLP-системы, такие как , Infowatch, SecureTower, SearchInform и другие. Функционал систем различен, поэтому организация при выборе системы должна четко понимать какие потоки информации ей необходимо защищать и решить каким функционалом можно пренебречь в пользу более важного.

Заключение:

После теоретического анализа различных статей можно сделать вывод, что вопрос о защите информации и защите от утечек конфиденциальной информации как никогда актуален. Дистанционная работа отличается от обычного формата деятельности, рабочие места более уязвимы. Поэтому компании должны применять в защите своих данных наиболее надежные способы и меры обеспечения информационной безопасности. Одним из таких систем являются DLP-системы-ПО, которое защищает секретные данные от утечек.

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 рекомендациями и мерами защиты информации при удаленной работе. Познакомился с DLP-системами, их функциями, составом, способами работы. 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.Логинова Е.В. Обеспечение информационной безопасности коммерческого предприятия при переводе сотрудников на удаленную работу. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=44196784 (дата обращения: 17.07.2021)

2. Афанасьева Д.В. Информационная безопасность при удаленной работе. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=46327373 (дата обращения: 20.07.2021)

3. А.А. Бутин, А.Н. Василевская. Обзор основных рекомендаций по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=43074426 (дата обращения: 17.07.2021)

4.Байрушин Ф.Т., Хлестова Д.Р. DLP-системы на предприятии как главное средство предотвращения утечки информации. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=27195705 (дата обращения: 23.07.2021)

5.Герцен Д.М., Стафьев А.В., Сердюков Н.В. Обзор DLP-систем. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=35276330 (дата обращения: 25.07.2021)

6.Чернокнижный Г.М., Никулина В.М., Образцова С.В. Опыт внедрения DLP-системы Falcongaze SecureTower на предприятиях. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=36553677 (дата обращения: 23.07.2021)