Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/nauchno-issledovatel'skaya-rabota/200437>

Тип работы: Научно-исследовательская работа

Предмет: Информационные технологии

Введение 3

1. Изучение существующих исследований в области противодействия внутренним нарушителям 5
 2. Определение сущности нарушителя и его целей в зависимости от области его существования 11
 3. Анализ основных методов идентификации нарушителя 15
 4. Направления применения методов противодействия внутреннему нарушителю в организации 24
- Заключение 29
- Список использованных источников 32
- Приложения 36

Введение

Стратегией развития информационного общества в РФ на 2017–2030 гг. в виде приоритетной траектории внутренней политики предусмотрено развитие информационных и коммуникационных технологий, образование информационного поля и инфраструктуры. С каждым годом информационные технологии глубже проникают в жизнь граждан. За последние годы в России на 100 человек приходится более 159 мобильных телефонов, из 100 человек 71 используют мобильный доступ к сети Интернет. Средняя скорость в сети Интернет выросла на 29 %, что поставило Россию на один уровень с Италией, Францией, Грецией. Глобальные изменения в сфере информационных процессов не могли не сказаться на состоянии информационной безопасности. Актуальность темы научно-исследовательской работы обусловлена тем, что знание и понимание информационной безопасности даёт возможность более тщательно вникнуть в правовые основы функционирования гражданского общества и государства. Информационная безопасность определяет степень достижения безопасности социума.

Степень изученности темы исследования представлены в трудах следующих авторов: А.П. Баранова, Т.А. Биячуева, Дж. Форрестер, А.С. Зайцева, А. А. Малюк, Н.Г. Милославской и других.

Объектом исследования являются внутренние нарушители в информационной безопасности.

Предметом – изучение методов противодействия внутреннему нарушителю.

Цель исследования – изучение возможностей внутреннего нарушителя и потенциальной опасности содержащей его сети.

Для достижения сформулированной цели рассмотрены и решены следующие задачи:

- изучить существующие исследования в области противодействия внутренним нарушителям;
- определить сущность нарушителя и его целей в зависимости от области существования;
- провести анализ основных методов идентификации нарушителя;
- определить направления применения методов противодействия внутреннему нарушителю в организации.

Методологическая основа исследования. В процессе изучения данной теме были использованы такие методы исследования как: классификация и синтез, сравнение и обобщение.

Практическая значимость работы состоит в исследовании возможностей внутреннего нарушителя, потенциальной опасности содержащей его сети, а также определении направлений применения методов противодействия внутреннему нарушителю в организации. Полученные данные могут быть применены для дальнейшего исследования проблемных вопросов в данном направлении.

Научно-исследовательская работа состоит из введения, трех глав, заключения, списка использованных источников и приложений.

1. Изучение существующих исследований в области противодействия внутренним нарушителям

В эпоху до повсеместного распространения интернет-технологий для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге. В настоящее время все чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же:

специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

А.П. Баранов выделяет, что информационная безопасность отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции их называют принципами информационной безопасности. Конфиденциальность означает, что доступ к информации есть только у того, кто имеет на это право. Например, пароль от электронной почты знает только пользователь и только он может читать свои письма. Если кто-то узнает пароль или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

Т.А. Биячуев выделил, что целостность означает сохранность информации сохраняется в полном объеме. Например, на электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

Доступность означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, пользователь в любой момент может войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной – только отдельные лица. Основные виды конфиденциальной информации представлены в таблице 1.

Таблица 1 – Основные виды конфиденциальной информации

№ п/п Понятие Краткое описание

- 1 Персональные данные Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные.
- 2 Коммерческая тайна Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.
- 3 Профессиональная тайна Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности.
- 4 Служебная тайна Информация, которая известна отдельным службам, например, налоговой или ЗАГС. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.
- 5 Государственная тайна Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные – к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Термин «информационная безопасность» может иметь различный смысл и трактовку в зависимости от контекста. Основные понятия, входящие в структуру этого термина представлены в табл.2.

Таблица 2 – Уровни законности

№ п/п Понятие Краткое описание

- 1 Конфиденциальность Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие право.
- 2 Целостность Состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется преднамеренно субъектами, имеющими право.
- 3 Доступность Состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно
- 4 Угрозы информационной безопасности Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
- 5 Атака Попытка реализации угрозы. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест в информационной системе. Они могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям (см. рис.1).

Рис.1. Угрозы информационной безопасности

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации (см. рис.2).

Рис.2. Уровни защиты информации

В российском законодательстве базовым законом в области защиты информации является ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года номер 149-ФЗ (ред. от 02.07.2021 № 355-ФЗ). Законодательный уровень представляет из себя основу для выстраивания структуры защиты информации, формирует основные понятия предметной области и выделяет меру наказания для возможных злоумышленников. Данный уровень имеет направляющую и координирующую роль, позволяет поддерживать в социуме карательное и негативное отношение к людям, которые нарушают законы информационной безопасности.

Исследования А. С. Зайцева и А. А. Малюка демонстрируют, что цифровые технологии прочно вошли в нашу жизнь, в бизнес. Проблемы безопасности данных выходят на первый план. Руководители осознают важность информационной безопасности (ИБ) для нормального функционирования организации. Анализируя актуальность изучения проблемы внутреннего нарушителя в организации, можно выделить, что аспекты, образующие информационную безопасность постоянно меняются, а масштабы и скорость этой эволюции возрастают. Антивирусные решения, основанные на специфических сигнатурах, универсальном и эвристическом обнаружении, недостаточны для того, чтобы справиться с потоком новых, очень сложных вариантов вредоносных программ, которые продолжают заражать системы компаний с более низким уровнем защиты.

Например, в антивирусной лаборатории PandaLabs компании PandaSecurity в 2019 году зарегистрировали и проанализировали 14,9 миллионов вредоносных событий, остановив 7,9 миллионов потенциально нежелательных программ (ПНП), а также 76 000 предупреждений об эксплоитах, предназначенных для использования уязвимостей в приложениях, сетях или оборудовании.

В I квартале 2020 года объем операций без согласия клиента вырос на 38% по сравнению с аналогичным периодом 2019 года на фоне двукратного снижения общего объема операций с использованием электронного средства платежа. Наиболее вероятная причина – начало использования дистанционных способов оплаты товаров и услуг той частью населения, которая до введения ограничений в связи с пандемией COVID-19 приобретала и оплачивала их непосредственно в точках продаж. В силу отсутствия необходимого опыта противодействия злоумышленникам эта категория граждан оказалась особенно уязвима к социальной инженерии.

По той же причине во II-м квартале 2020 года наблюдалось дальнейшее увеличение объема операций без согласия клиента (+59%) на фоне роста общего объема операций с использованием электронного средства платежа. Перевод на удаленный режим работы способствовал ряду хищений в системах ДБО юридических лиц в I и II кварталах 2020 года. Об этом свидетельствует рост доли хищений с применением социальной инженерии при сокращении числа таких операций, росте их общего объема и снижении доли возмещения (в I квартале 2020 года).

Эти данные демонстрируют, что в любой ИТ-среде существует слишком много угроз и векторов атак, которые могут привести к нарушению. Сегодня решения в области информационной безопасности должны быть предсказуемыми, проактивными, готовыми реагировать на любой инцидент, который может возникнуть.

Фактически, внутренние нарушители информационной безопасности преследуют три цели, представленные на рис.3.

Рис.3. Цели, преследуемые нарушителями информационной безопасности

Службы должны учитывать особенности современных технологий при планировании мероприятий по обеспечению информационной безопасности.

Таким образом информационная безопасность – это защита и сохранение информации, а также её значимых элементов, в том числе системы оборудования, которая предназначена для применения, сбережения и передачи информации. Другими словами, это перечень стандартов, технологий и методов управления, необходимых для защиты информационной безопасности.

2. Определение сущности нарушителя и его целей в зависимости от области его существования

Определение сути нарушителя и его целей зависит от вида угрозы для информационной безопасности. Соответственно, определение сущности нарушителя и его целей целесообразно проводить при помощи моделирования каждой из внутренних угроз отдельно. Классификация внутренних нарушителей, разработанная А.С. Зайцевым и А.А. Малюковым представлена в таблице 3.

Таблица 3. Классификация внутренних угроз ИБ

Внутренняя угроза ИБ Мотив

Нарушителя Предполагается

увольнение Сговор внутренний Сговор внешний

1 2 3 4 5

Саботаж Обида Не всегда Нет Нет

Шпионаж Деньги

Обида Нет Нет Да

Мошенничество на руководящей должности Деньги Нет Нет

Социальная инженерия Нет

Мошенничество на неруководящей должности Деньги Нет Нет Не всегда

Продолжение таблицы 3

1 2 3 4 5

Кража ИСБ в целях получения деловых преимуществ в одиночку Бизнес-преимущества

Обида Да Нет Да

1. Конституция Российской Федерации от 12 декабря 1993 г.: по сост. на 21 июля 2014 г. // Собрание законодательства Российской Федерации. – 2020. - № 16 . – Ст. 445.

2. Уголовный кодекс Российской Федерации: принят Гос. Думой от 24.05.1996 № 63-ФЗ (ред. от ред. от 01.07.2021 № 292-ФЗ,) [Электронный ресурс] // Справ.- правовая система «КонсультантПлюс». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021 № 355-ФЗ) [Электронный ресурс] // Справ.- правовая система «КонсультантПлюс». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс].URL: http://www.consultant.ru/document/cons_doc_LAW_216363/

5. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс].

URL:<https://normativ.kontur.ru/document?moduleId=1&documentId=197897>

6. ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью»[Электронный ресурс]. URL:<https://docs.cntd.ru/document/1200044724>

7. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

8. Баранов А. П. Актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения // Вопросы кибербезопасности. 2015. №1 (9). URL: <https://cyberleninka.ru/article/n/aktualnye-problemy-v-sfere-obespecheniya-informatsionnoy-bezopasnosti-programmnogo-obespecheniya>

9. Биячурев Т.А. Безопасность корпоративных сетей. Санкт-Петербург, 2004.

10. Высокопроизводительная DLP-система для блокирования утечек информации, контроля коммуникаций сотрудников и выявления признаков корпоративного мошенничества [Электронный ресурс].URL:<https://clck.ru/YVuDd>

11. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

12. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. – С.54

13. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие : в 2 ч. / [А. В. Аносов и др.]. –

М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.

14. Ефимова, Л.Л. Информационная безопасность. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — С.94
15. Зайцев А. С., Малюк А. А. Исследование проблемы внутреннего нарушителя // История и архивы. 2012. №14 (94). URL: <https://cyberleninka.ru/article/n/issledovanie-problemy-vnutrennego-narushitelya-1>
16. Зайцев А.С. Анализ подходов к решению проблемы противодействия инсайдерским угрозам информационной безопасности [Электронный ресурс] / А. С. Зайцев, А. А. Малюк // Вестник РГГУ. - 2015. - № 12. - С. 21-36.
17. Зайцев А.С. Разработка классификации внутренних угроз информационной безопасности посредством кластеризации инцидентов [Электронный ресурс] / А. С. Зайцев, А. А. Малюк // Безопасность информационных технол. - 2016. - № 3. - С. 20-33.
18. Зайцев А.С. Разработка классификации внутренних угроз информационной безопасности посредством кластеризации инцидентов [Электронный ресурс] / А. С. Зайцев, А. А. Малюк // Безопасность информационных технол. - 2016. - № 3. - С. 20-33.
19. Зайцев А.С. Системно-динамическое моделирование угрозы кражи интеллектуальной собственности [Электронный ресурс] / А. С. Зайцев, А. А. Малюк // Научная визуализация. - 2015. - № 3. - С. 53-68.
20. Зайцев А.С. Системно-динамическое моделирование угрозы кражи интеллектуальной собственности [Электронный ресурс] / А. С. Зайцев, А. А. Малюк // Вестник РГГУ. - 2015. - № 12. - С. 70-91.
21. Инсайдерские угрозы в России 2009 [Электронный ресурс] // Сайт Perimetrix. [М., 2009]. URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf
22. Милославская Н.Г. Identifying a Potential Insider Using Classification Models [Электронный ресурс] / А. С. Зайцев, А. А. Малюк, Н.Г. Милославская // Automatic Control and Computer Sciences. - 2017. - № 83. - С. 860-866.
23. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс].URL:https://cbr.ru/analytics/ib/review_1q_2q_2020/
24. Отчет «Понимание кибер-угроз 2020»[Электронный ресурс].URL: https://cbr.ru/analytics/ib/review_1q_2q_2020/
25. Форрестер Дж. Основы кибернетики предприятия. – М.: Прогресс, 1971.
26. Что такое информационная безопасность и какие данные она охраняет [Электронный ресурс].URL: <https://habr.com/ru/users/pandasecurityrus/posts/>
27. 43 статистических факта про ИБ вовремя COVID-19 [Электронный ресурс].URL: <https://zen.yandex.ru/media/mcs/chto-takoe-informacionnaia-bezopasnost-i-kakie-dannye-ona-ohraniaet-5eece558d17b0f4662264771>
28. Cressey D.R. Other People's Money – Wadsworth, 1974.
29. Yin R.K. Case Study Research 3rd ed. – Thousand Oaks: Sage Publications, 2003.
30. LexisCourtDatabase [Электронный ресурс] Режим доступа к ресурсу: <http://www.lexis.com>.
31. CyberSecurityWatch Survey [Электронный ресурс] // Сайт Carnegie Mellon University. [М., 2011]. URL: http://www.cert.org/archive/pdf/Cyber_SecuritySurvey2011Data.pdf
32. CERT SocieteGenerale [Электронный ресурс]. URL: <http://dorlov.blogspot.com/2011/11/cert.html>

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/nauchno-issledovatel'skaya-rabota/200437>