www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.4.4

УДК 004.056
ББК 32.971.35

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

Наталья Алексеевна Головачева

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
golovacheva.natalya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Россия

Мария Дмитриевна Маслакова

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
BIT-201_212274@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Россия

Аннотация. В статье проведен анализ киберпреступлений и методов защиты от них в сети Интернет. Выделены критерии для адекватной оценки методов защиты от киберпреступлений в сети Интернет. И в рамках экспериментальных исследований выявлен наилучший метод защиты, учитывая требования и потребности пользователя.

Ключевые слова: киберпреступность, компьютерные преступления, хакинг, кибератака, антивирусное программное обеспечение, межсетевой экран, криптографическое средство защиты информации, средства обнаружения вторжений.

Современные технологии стали частью нашей повседневной жизни, предоставляя нам множество удобств и возможностей. В процессе использования этих технологий, мы часто забываем о рисках потери конфиденциальности.

Каждый из нас либо сам сталкивался, либо слышал о случаях мошенничества в Интернете. С каждым годом все больше людей подвергаются атакам онлайн-мошенников. Также наблюдается увеличение онлайн-активности экстремистских, террористических и противозаконных сообществ в сети. Мы сталкиваемся с анонимностью, случаями манипулирования информацией в Интернете (например, секстингом и кибербуллингом), развитием новых форм девиантного поведения и молодежных криминальных субкультур в виртуальном мире. Из-за быстрого развития технологий необходимо анализировать развитие преступлений в киберпространстве.

За последние годы [2] чаще всего жертвами кибератак становились государственные и медицинские учреждения. Нередки нападения на промышленные организации, а также на объекты критической инфраструктуры и системы водоснабжения. Страдают от нападений киберпреступников и частные пользователи, использующие сеть Интернет. Самыми распространенными методами кибератак являются ВПО и соци-

альная инженерия. С момента начала пандемии COVID-19 в 2020 г. стал все активнее использоваться хакинг, включая атаки на цепочки поставок.

Количество уникальных киберинцидентов растет из года в год (в 2020 г. выросло на 51 % по сравнению с 2019 г.), причем большая часть носит целенаправленный характер [1]. Киберпреступники часто прибегают к подготовительному этапу для более крупных мошеннических схем, который сопровождается сложными многоступенчатыми техниками, включающими несколько методов в рамках одной атаки. Данная схема используется для закрепления в системе и увеличения возможности как можно дольше оставаться незамеченным. В результате существенно увеличивается количество атак, основными мотивами которых являются кража или несанкционированное получение информации и финансовая выгода.

Выделим критерии, по которым можно классифицировать киберпреступления по объекту:

1. Киберпреступления, связанные с компьютерами и сетями: атаки на компьютерные системы, включая взломы, вирусы, черви, трояны и другие вредоносные программы. Целью таких киберпреступлений является получение незаконного доступа, кража данных или повреждение системы.

2. Киберпреступления, связанные с электронной коммерцией: мошенничество в онлайн-торговле, фишинг и другие виды мошенничества, связанные с финансовыми операциями в интернете.

3. Киберпреступления, связанные с личной информацией пользователей: нарушение конфиденциальности личных данных, в том числе утечки информации о платежных картах, медицинские данные и другую личную информацию.

4. Киберпреступления, связанные с государственными системами: кибершпионаж и хакерские атаки на государственные организации, правительственные сайты и объекты.

5. Киберпреступления, связанные с промышленными предприятиями и критической инфраструктурой, атаки на энергетические системы, системы водоснабжения, транспортные сети и другие критически важные объекты, имеющие значительное влияние на функционирование общества.

6. Киберпреступления, связанные с социальными сетями и онлайн-платформами: массовые атаки на аккаунты, распространение информации неправомерного содержания и дискриминацию.

В рамках экспериментальных исследований анализируются следующие методы защиты от вышеуказанных киберпреступлений (см. табл. 2):

1. Антивирусное программное обеспечение.

2. Межсетевой экран.

3. Контроль и управление доступом.

4. Криптографическое средство защиты информации.

5. Средство обнаружения вторжений, средство обнаружения атак: программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности [4].

6. Виртуальные частные сети (VPN).

7. Аудит безопасности.

8. Сложные пароли – это главный барьер, который защищает наши данные от злоумышленников. Пароль считается сложным, если:

1) его длина не менее 12 символов;

2) в нем используются специальные знаки, например !, или ?, или % и т. д.;

3) использованы строчные и прописные буквы;

4) использована кодовая фраза, использующая несколько несвязанных по смыслу слов [3].

При анализе методов защиты от киберпреступлений необходимо ввести следующие критерии оценки:

1. Эффективность: критерий определяет, насколько хорошо метод защиты способен предотвратить, обнаружить или остановить киберпреступление (К1).

2. Надежность: критерий определяет, насколько надежно метод защиты способен действовать в широком диапазоне условий и ситуаций (К2).

3. Удобство использования: критерий определяет, насколько метод защиты легко внедрить и использовать. Он должен быть интуитивно понятным, простым в настройке и использовании, а также не причинять излишних неудобств для пользователей (К3).

4. Масштабируемость: критерий определяет, насколько метод защиты способен применяться в различных сетевых средах и организациях (К4).

5. Совместимость: критерий определяет, насколько метод защиты совместим с другими системами, аппаратным и программным обеспечением (К5).

6. Стоимость: критерий определяет экономическую стоимость внедрения и поддержки метода защиты (К6).

7. Гибкость и адаптивность: критерий определяет, насколько метод защиты способен адаптироваться к новым и развивающимся угрозам и технологиям (К7).

8. Соответствие стандартам безопасности: критерий определяет, насколько метод должен соответствовать требованиям и стандартам безопасности, чтобы гарантировать эффективную защиту от киберпреступлений (К8).

9. Прозрачность: критерий определяет, насколько метод защиты понятен и открыт для аудита, проверки и исследования экспертами в области кибербезопасности (К9).

В таблице 1 приведены качественные характеристики критериев оценки.

Поскольку ни один из рассматриваемых методов не удовлетворяет оптимально всем критериям, требуется разработка программного инструмента для автоматического выбора наилучшего метода защиты от киберпреступлений в сети Интернет.

Таблица 1

Качественные характеристики критериев оценки

№	Критерий	Значение		
К1	Эффективность	низкая	средняя	высокая
К2	Надежность	низкая	средняя	высокая
К3	Удобство использования	сложно	умеренно	легко
К4	Масштабируемость	низкая	средняя	высокая
К5	Совместимость	отсутствует	частичная	бесшовная
К6	Стоимость	дорогая	умеренная	доступная
К7	Гибкость и адаптивность	низкая	средняя	высокая
К8	Соответствие стандартам безопасности	не соответствует		соответствует
К9	Прозрачность	низкая	средняя	высокая

Таблица 2

Значения критериев оценки для каждого метода защиты

Метод защиты	Критерий								
	К1	К2	К3	К4	К5	К6	К7	К8	К9
Антивирусное программное обеспечение	высокая	высокая	легко	средняя	частичная	умеренная	средняя	соответствует	высокая
Межсетевые экраны	высокая	высокая	легко	высокая	частичная	умеренная	высокая	соответствует	высокая
Контроль и управление доступом	высокая	средняя	умеренно	высокая	бесшовная	доступная	средняя	соответствует	высокая
Средства криптографической защиты информации	высокая	средняя	умеренно	высокая	бесшовная	доступная	низкая	соответствует	средняя
Средства обнаружения вторжений	высокая	высокая	умеренно	высокая	бесшовная	умеренная	высокая	соответствует	высокая
Виртуальные частные сети (VPN)	высокая	средняя	умеренно	средняя	частичная	доступная	средняя	соответствует	средняя
Аудит безопасности	средняя	средняя	легко	высокая	бесшовная	доступная	средняя	соответствует	высокая
Использование сложных паролей	средняя	высокая	умеренно	высокая	бесшовная	доступная	высокая	соответствует	низкая

Была разработана математическая модель оценки методов защиты от киберпреступлений в сети Интернет, с помощью которой можно рассчитать обобщенный показатель критериев исходя из полученных требований. Разработана архитектура программного средства оценки методов защиты от киберпреступлений в сети Интернет.

Экспериментальные исследования по поиску наилучшего метода защиты от киберпреступлений в сети интернет были проведены для трех случаев:

1. На вход программного средства подаются низкие требования к методу защиты от киберпреступлений.

2. На вход программного средства подаются средние требования к методу защиты от киберпреступлений.

3. На вход программного средства подаются высокие требования к методу защиты от киберпреступлений.

В ходе анализа экспериментальных исследований была составлена таблица 3 для обобщения полученных результатов.

По результатам проведенных экспериментальных исследований можно сделать вывод, что программное средство успешно определяет наилучший метод защиты от киберпреступлений в сети Интернет, учитывая требования и потребности пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: итоги 2020 года // Лидер результативной кибербезопасности. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. – Загл. с экрана.

2. Актуальные киберугрозы: I квартал 2023 года // Лидер результативной кибербезопасности. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1/. – Загл. с экрана.

3. Надежные пароли: как их создать и чем они полезны? // Лаборатория Касперского. – Электрон. текстовые дан. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/how-to-create-a-strong-password. – Загл. с экрана.

4. Средства обнаружения и предотвращения вторжений // ООО «ПНК». – Электрон. текстовые дан. – Режим доступа: https://www.y-center.ru/corporate/zaschita-informatsii/sredstva-zaschity-

Таблица 3

Результаты экспериментальных исследований

№ п/п	Требования	Полученные оценки	Наилучший метод
1	Низкие требования по каждому критерию	Антивирусное программное обеспечение – 2 Межсетевые экраны – 2 Контроль и управление доступом – 2 Средства криптографической защиты информации – 1 Средства обнаружения вторжений – 2 Виртуальные частные сети (VPN) – 2 Аудит безопасности – 2 Сложные пароли – 2	Все перечисленные, кроме средств криптографической защиты информации
2	Средние требования по каждому критерию	Антивирусное программное обеспечение – 5 Межсетевые экраны – 5 Контроль и управление доступом – 4 Средства криптографической защиты информации – 4 Средства обнаружения вторжений – 5 Виртуальные частные сети (VPN) – 6 Аудит безопасности – 4 Сложные пароли – 4	Виртуальные частные сети (VPN)
3	Высокие требования по каждому критерию	Антивирусное программное обеспечение – 5 Межсетевые экраны – 7 Контроль и управление доступом – 6 Средства криптографической защиты информации – 5 Средства обнаружения вторжений – 7 Виртуальные частные сети (VPN) – 3 Аудит безопасности – 6 Сложные пароли – 6	Межсетевые экраны и средства обнаружения вторжений

informatsii/obnaruzheniya-predotvrashcheniya-vtorzheniy/. – Загл. с экрана.

REFERENCES

1. Aktualnye kiberugrozy: itogi 2020 goda [Current Cyber Threats: 2020 Results]. *Lider rezultativnoj kiberbezopasnosti* [Effective Cyber Security Leader]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

2. Aktualnye kiberugrozy: I kvartal 2023 goda [Current Cyber Threats: Q1 2023]. *Lider rezultativnoj kiberbezopasnosti* [Effective Cyber Security Leader]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1/

3. Nadezhnye paroli: kak ih sozdat i chem oni polezny? [Strong Passwords: How to Create Them and What Are They Useful For?]. *Laboratorija Kasperskogo* [Kaspersky Lab]. URL: https://www.kaspersky.ru/resource-center/threats/how-to-create-a-strong-password

4. Sredstva obnaruzhenija i predotvrashhenija vtorzhenij [Intrusion Detection and Prevention Tools]. *OOO «PNK»* [PNK Ltd.]. URL: https://www.y-center.ru/corporate/zaschita-informatsii/sredstva-zaschity-informatsii/obnaruzheniya-predotvrashcheniya-vtorzheniy/

RESEARCH OF METHODS OF PROTECTION AGAINST CYBERCRIME ON THE INTERNET

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
golovacheva.natalya@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Maria D. Maslakova

Student, Department of Information Security,
Volgograd State University
BIT-201_212274@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Modern technologies have become a part of our daily livesz, providing us with many amenities and opportunities. In the process of using these technologies, we often forget about the risks of losing privacy. Smartphones, tablets, and laptops – all these devices can track our actions and disclose a lot of information about us, especially when using certain programs and services. The urgency of this problem is evidenced by the increase in crimes in cyberspace. We are increasingly hearing in the news about cases of fraud on the Internet. More and more people are being attacked by online scammers. There is also an increase in the online activity of extremist, terrorist, and illegal communities on the network. We face anonymity, cases of manipulation of information on the Internet (for example, sexting and cyberbullying), the development of new forms of deviant behavior, and youth criminal subcultures in the virtual world. Due to the rapid development of technology, it is necessary to analyze the development of crimes in cyberspace.

The article analyzes cybercrime and methods of defense against it on the Internet. Criteria for an adequate evaluation of methods of protection against cybercrime on the Internet are identified. And within the framework of experimental research, the best method of protection is determined, taking into account the requirements and needs of the user.

Key words: cybercrime, computer crimes, hacking, cyberattack, antivirus software, firewall, cryptographic information security, intrusion detection tools.