УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ БЕЛАРУСЬ: УГРОЗЫ И ЗАЩИТНЫЕ МЕРЫ

Шуляк Я.А., Романюк М.С., Степанчук Д.Е.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Воробей А.В. – магистр технических наук, ассистент кафедры ИПиЭ

Аннотация. В современном мире защита информации в сфере информационной безопасности (InfoSec) стала одним из важнейших приоритетов из-за увеличения зависимости от технологий и интернета. Информационная безопасность (InfoSec) охватывает инструменты и процессы, используемые организациями для защиты конфиденциальной информации. Она включает меры предотвращения несанкционированного доступа, проверки, изменения, записи, нарушения или уничтожения данных. Развитие и поддержание мер информационной безопасности необходимо для защиты конфиденциальных данных, таких как данные клиентов, финансовые данные или интеллектуальная собственность, от кражи, подделки и разрушения.

Ключевые слова: информационная безопасность, киберпреступность, кибербезопастность, Республика Беларусь, государственная политика.

Введение. В настоящее время информационная безопасность становится одним из ключевых аспектов, поскольку зависимость от технологий и интернета постоянно растет. Угрозы кибератак и утечек данных требуют принятия мер и практик для защиты конфиденциальности, целостности и доступности информации. Информационная безопасность, иногда обозначаемая как InfoSec, охватывает широкий спектр инструментов и процессов, предназначенных для защиты данных от несанкционированного доступа и использования.

Основная часть. Рассмотрим подробнее, что же такое информационная безопасность. Информационная безопасность (иногда называемая InfoSec) охватывает инструменты и процессы, которые организации используют для защиты информации. Сюда входят настройки политики, которые предотвращают доступ неавторизованных лиц к деловой или личной информации. InfoSec – это растущая и развивающаяся область, охватывающая широкий спектр областей: от безопасности сетей и инфраструктуры до тестирования и аудита. Цель состоит в том, чтобы обеспечить безопасность и конфиденциальность критически важных данных, таких как данные счетов клиентов, финансовые данные или интеллектуальная собственность.

В современном мире существует множество угроз информационной безопасности, включая хакерские атаки, фишинг, вредоносное ПО и внутренние угрозы. Эти угрозы могут иметь серьезные последствия для отдельных лиц, организаций и даже целых государств. Для борьбы с этими угрозами применяются различные защитные меры, такие как шифрование, контроль доступа, брандмауэры и антивирусное программное обеспечение. Кроме того, организации разрабатывают политики и процедуры для повышения культуры осведомленности о безопасности и соблюдения среди сотрудников [1].

Несмотря на эти усилия, постоянно меняющаяся природа киберугроз требует бдительности и обновления мер безопасности. Кроме того, сотрудничество и обмен информацией между правительствами, организациями и отдельными лицами важны для решения глобальной проблемы информационной безопасности. Поскольку технологии продолжают развиваться, защита информационной безопасности останется одним из главных приоритетов в современном мире. Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент

программы информационной безопасности должен быть разработан для реализации одного или нескольких из этих принципов. Вместе они называются Триадой ЦРУ.

Рассмотрим данные принципы подробнее.

1. Конфиденциальность

Меры конфиденциальности призваны предотвратить несанкционированное раскрытие информации. Целью этого принципа является сохранение конфиденциальности личной информации и обеспечение ее видимости и доступа только тем лицам, которые владеют ею или нуждаются в ней для выполнения своих организационных функций.

2. Честность

Согласованность включает защиту от несанкционированных изменений (добавок, удалений, изменений) данных. Принцип целостности гарантирует, что данные точны и надежны и не изменяются неправильно, случайно или злонамеренно.

3. Доступность

Доступность – это защита способности системы обеспечивать полную доступность программных систем и данных, когда это необходимо пользователю (или в определенное время). Цель доступности – сделать технологическую инфраструктуру, приложения и данные доступными, когда они необходимы для организационного процесса или для клиентов организации [1].

Угрозы и атаки информационной безопасности – это действия или события, которые могут поставить под угрозу конфиденциальность, целостность или доступность данных и систем. Они могут возникать из различных источников, таких как отдельные лица, группы или даже природные явления. Вот некоторые распространенные угрозы и атаки информационной безопасности:

1. Атака вредоносного ПО

Атаки, использующие социальную инженерию или уязвимости в браузерах и операционных системах, позволяют злоумышленникам устанавливать вредоносное ПО на устройства пользователей, которое может отслеживать и отправлять конфиденциальные данные, участвовать в бот-сетях и помогать злоумышленникам проникать в другие цели в сети.

2. Атаки социальной инженерии

Атаки социальной инженерии основаны на психологическом манипулировании пользователями, заставляя их выполнять действия, желаемые злоумышленником, или разглашать конфиденциальную информацию.

3. Атаки на цепочку поставок программного обеспечения

Атака на цепочку поставок программного обеспечения направлена на уязвимости в доверенных обновлениях программного обеспечения и цепочке поставок, используя доверие организаций к сторонним поставщикам, особенно в отношении обновлений и исправлений, что особенно актуально для сетевого мониторинга, промышленных систем управления и других сетевых систем.

4. Расширенные постоянные угрозы (APT)

Когда человек или группа получает несанкционированный доступ к сети и остаются незамеченными в течение длительного периода времени, злоумышленники могут украсть конфиденциальные данные, намеренно избегая обнаружения сотрудниками службы безопасности организации. APT требуют от злоумышленников опытных и серьезных усилий, поэтому их обычно используют против национальных государств, крупных корпораций или других очень ценных целей.

5. Распределенный отказ в обслуживании (DDoS)

Цель DoS-атаки – перегрузить ресурсы целевой системы и лишить доступа пользователей, а DDoS – это вариант DoS, при котором злоумышленники компрометируют множество устройств для координированной атаки. DDoS-атаки часто используются в сочетании с другими киберугрозами, чтобы привлечь внимание служб безопасности и осуществлять более тонкие атаки.

6. Атака «Человек посередине» (MitM)

Когда пользователи или устройства получают доступ к удаленной системе через Интернет, они предполагают, что общаются напрямую с сервером целевой системы. При атаке MitM злоумышленники нарушают это предположение, ставя себя между пользователем и целевым сервером. Как только злоумышленник перехватит сообщения, он сможет скомпрометировать учетные данные пользователя, украсть конфиденциальные данные и вернуть пользователю различные ответы.

7. Атаки на пароли

Хакер может получить доступ к информации о пароле человека, «перехватив» соединение с сетью, используя социальную инженерию, угадав или получив доступ к базе данных паролей. Злоумышленник может «угадать» пароль случайным или систематическим образом [2].

Целью государственной политики обеспечения информационной безопасности в Республике Беларусь является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

В рамках политики информационной безопасности Республики Беларусь применяются следующие направления:

1. На государственном уровне проводится мониторинг информационной безопасности, определяются приоритеты для предотвращения угроз и минимизации их воздействия. Разрабатываются меры для нейтрализации информационных рисков и угроз.

2. Гражданам обеспечивается свобода информации, защита личной жизни, персональных данных и авторских прав. Соблюдается баланс прав с ограничениями для национальной безопасности. Создаются условия для безопасности национальных СМИ, осуществляется контроль их деятельности.

3. Реализуется максимальная доступность для граждан и организаций государственных электронных услуг, административных процедур и информационных ресурсов государственных органов и организаций.

4. Повышается осведомленность граждан и общества об угрозах национальной безопасности и государственных мерах по ее обеспечению, их вовлеченность в обеспечение безопасности информационной сферы.

5. Государство поддерживает защиту национальных информационных систем и безопасность программного обеспечения. Для улучшения устойчивости к информационным рискам используются передовые технологии и новые средства обеспечения безопасности.

6. Деяния, угрожающие информационной безопасности, криминализируются. Принимаются меры против киберпреступности и кибертерроризма. Вводятся правовые режимы безопасности информации и проводится ответственность за вред государственным информационным системам.

7. Создаются средства для информационной безопасности, увеличивается научный потенциал и финансирование для новых решений в этой области. Разрабатываются инновационные методы защиты информации.

Основными источниками угроз в области обеспечения безопасности информационных ресурсов в Республике Беларусь следует рассматривать деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях, осуществляемого в обход установленного порядка или вопреки общепринятым нормам морали и нравственности, а также нарушение функционирования информационной инфраструктуры.

Основной целью государственной политики в области обеспечения безопасности информационных ресурсов является сохранение их доступности, целостности и конфиденциальности. Система обеспечения безопасности информационных ресурсов основана на стратегическом принципе соблюдения баланса свободы информации и права на тайну, гарантиях государства на распространение или предоставление общедоступной информации. Государство обеспечивает расширение безопасного доступа к информационным ресурсам добросовестных пользователей, развитие сервисов качественного и удобного предоставления информации, совершенствование систем ее данных [3].

Заключение. Информационная безопасность остается ключевым аспектом в современном мире, где технологии продолжают развиваться, а угрозы информационной безопасности становятся более сложными и изощренными. Важность сотрудничества и обмена информацией между государствами, организациями и отдельными лицами необходима для успешного противостояния угроз информационной безопасности. Стратегии и меры безопасности, такие как шифрование, контроль доступа и обучение сотрудников, остаются неотъемлемой частью защиты, а совместные усилия могут способствовать разработке более эффективных стратегий и обеспечению общей безопасности.

Список литературы

1. What is information Security(InfoSec) – Режим доступа: https://www.imperva.com/learn/data-security/information-security-infosec/ - Дата доступа: 13.11.2023

2. What are the principles of information security – Режим доступа: https://www.hackerone.com/knowledge-center/principles-threats-and-solutions / - Дата доступа: 16.11.2023

3. Концепция информационной безопасности Республики Беларусь – Режим доступа: https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html?amp=1/ - Дата доступа: 16.11.2023

4. Cyber security is an Essential Aspect Of Our Modern World – Режим доступа: https://www.linkedin.com/pulse/cyber-security-essential-aspect-our-modern-world-gary-o-neill-1e/ - Дата доступа: 25.11.2023

UDC 004.056

INFORMATION SECURITY IN THE REPUBLIC OF BELARUS: THREATS AND PROTECTIVE MEASURES

Shuliak Y.A., Ramaniuk M.S., Stepanchyk D.E.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vorobey A.V. – Master of Sci., Assistant of the Department of EPE

Annotation. In the modern world, the protection of information in the field of information security (InfoSec) has become one of the most important priorities due to increasing dependence on technology and the Internet. Information Security (InfoSec) covers the tools and processes used by organizations to protect confidential information. It includes measures to prevent unauthorized access, verification, modification, recording, violation or destruction of data. The development and maintenance of information security measures is necessary to protect sensitive data such as customer data, financial data or intellectual property from theft, forgery and destruction.

Keywords: information security, cybercrime, cybersecurity, The Republic of Belarus, state policy.