УДК 004

Скрипин Артем Игоревич, студент факультета ИТиАБД,
Направление подготовки: 10.03.01 Информационная безопасность
Финансовый университет при правительстве Российской Федерации, Москва
Skripin Artem Igorevich, Financial University under the Government
of the Russian Federation, Moscow

Барский Максим Евгеньевич, студент факультета ИТиАБД,
Направление подготовки: 10.03.01 Информационная безопасность
Финансовый университет при правительстве Российской Федерации, Москва
Barskiy Maxim Evgenievich, Financial University under the Government
of the Russian Federation, Moscow

Резниченко Сергей Анатольевич, канд. техн. наук, доцент,
Финансовый университет при правительстве Российской Федерации, Москва
Национальный исследовательский ядерный университет «МИФИ», Москва
Российский государственный университет нефти и газа (НИУ)
им. И. М. Губкина, Москва
Reznichenko Sergey Anatolievich, National Research Nuclear University
"MEPhI", (Moscow Engineering Physics Institute), Moscow
Gubkin Russian State University of Oil and Gas
(National Research University), Moscow

ПРОБЛЕМЫ И ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ УПРАВЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
PROBLEMS AND MAIN DIRECTIONS OF MANAGEMENT DEVELOPMENT IN THE FIELD OF INFORMATION SECURITY

Аннотация: Статья об информационной безопасности подчеркивает комплексный подход и три направления: технологии, организация и правовое регулирование. Важны использование соответствующего оборудования,

формирование структуры с опытными кадрами, определение правового статуса и мониторинг систем. Диагностика существующих систем для выявления уязвимостей также необходима.

Abstract: The article on information security emphasizes a comprehensive approach and three directions: technology, organization, and legal regulation. It is important to use appropriate equipment, establish a structure with experienced personnel, determine legal status, and monitor systems. Diagnostic assessment of existing systems to identify vulnerabilities is also essential.

Ключевые слова: система управления информационной безопасностью, информационная безопасность, системный подход, уязвимость, угроза, несанкционированный доступ.

Keywords: Information Security Management System, information security, systematic approach, vulnerability, threat, unauthorized access.

1. Введение

Современные понятия информационной безопасности включают в себя не только физические средства и программное обеспечение, но также организационно-правовые мероприятия, направленные на защиту данных от преднамеренных противоправных или случайных негативных воздействий. Использование системного подхода позволяет эффективно минимизировать возможные угрозы и обеспечить надежную защиту информационных систем.

При разработке конкретных рекомендаций по обеспечению информационной безопасности необходимо учитывать множество факторов. Важно учитывать тип угрозы, потенциальный ущерб, который она может нанести, а также принципы и критерии формирования информационной безопасности в организации. Это может включать разработку политик и процедур, обучение сотрудников, регулярный мониторинг и аудит информационных систем, установление правил доступа и контроля, а также резервное копирование и восстановление данных.

Поддержание информационной безопасности становится все более актуальным в современном цифровом мире, где информация является одним из наиболее ценных активов организаций. Эффективное управление информационной безопасностью становится приоритетом для обеспечения доверия, защиты конфиденциальности и сохранения бизнес-процессов.

2. Основная часть исследования

Принципы информационной безопасности

Независимо от сферы деятельности организации, система управления ее информационной безопасностью должна быть основана на следующих четырёх принципах:

1. Целостность. Способность информационной системы сохранять структуру и изначальный вид сохраняемых данных в полном объёме. При этом целостность должна соблюдаться, как при "статичном" хранение данных, так и при их неоднократной передаче различными средствами. Дополнять, редактировать или удалять данные может только пользователь с соответствующим доступом.

2. Доступность. Данные, которые, позиционируются, как информация в свободном доступе, должны предоставляться беспрепятственно, в полном объёме и своевременно. При условии, что запрос пришёл от пользователей ресурса, которые имеют соответствующие права.

3. Конфиденциальность. Параметр, определяющий ограничения доступа к информации. В процессе формирования политики конфиденциальности организации доступ к информационным ресурсам получает круг лиц, включённых в определённые списки и прошедших аутентификацию;

4. Достоверность. Определяет принадлежность источника информации владельцу или его доверенному лицу.

На основании перечисленных принципов формируется комплекс мер призванных выявлять, отслеживать, предотвращать или устранять

несанкционированный доступ к информационным ресурсам у лиц, не имеющих соответствующего разрешения. Также, эти меры должны предотвращать искажение, повреждение, несанкционированное копирование или блокировку сохраняемых или передаваемых данных.

Принципиальным требованиям является необходимость решения всех перечисленных задач одновременно. Только в этом случае система управления информационной безопасностью сможет обеспечить надёжную и полноценную защиту.

Классификация угроз информационной безопасности

Основные проблемы, с которыми сталкивается управление информационной безопасности, это разнообразные угрозы и уязвимости системы. Следует понимать, что угрозы не проявляются самостоятельно. Их можно выявить только через взаимодействие с определёнными факторами защитные системы, которые являются наиболее слабыми звеньями в цепи защиты, что и получило обозначение факторы уязвимости. Если проанализировать основные аспекты уязвимостей информационных систем, то можно привести их к совокупности следующих факторов:

- Несовершенство аппаратной платформы и программной оболочки. Как правило, проявляется в использовании морально устаревшего оборудования и программного обеспечения, неправильных настройках и конфигурациях, ошибках обслуживания и т. п.;
- Ошибки и неточности в протоколах передачи информации. Могут основываться, как на несовершенстве процессов функционирования, так и на использовании автоматизированных систем данных с разными характеристиками (несовместимость информационных потоков);
- Излишне сложные условия расположения, хранения, обработки и использования информации.

Главной причиной запускаемых угроз является нанесение ущерба информации или хищение данных (несанкционированное копирование) с целью

получения выгоды. Однако, возможно возникновение угроз из-за низкого уровня защиты, непрофессиональных действий пользователей, или других массовых факторов угрожающего характера.

Проанализировав статистику наиболее распространённых проблем, связанных с информационной безопасностью, можно классифицировать уязвимость следующим образом.

Объективные

Чаще всего зависят от технического состояния, структуры и эксплуатационных характеристик используемого оборудования. Полностью оптимизировать данные факторы для гарантированного устранения уязвимости невозможно. Но существует ряд методов, обеспечивающих, как частичное устранение угроз, так и снижение вероятности возникновения уязвимости.

1. Технические средства, в основном, связанные с устранением электромагнитного излучения от силовых кабельных линий и оборудования:

Использование экранированных кабелей, в правильном заземлении и занулении, аппаратные средства нейтрализации внешних электромагнитных наводок;

Электрические и акустические варианты обратной связи – представляют собой сигналы, передаваемые по электросети при возникновении / обнаружении внешних наводок, или неравномерных распределений параметров тока;

2. Программные средства:

Вирусы и прочие вредоносное ПО, которое проникает через систему безопасности, как самостоятельно, так и с использованием нелегальных / не лицензированных программ с "закладками" - не регламентируемыми выходами, и функциями сбора и коррекции данных;

Аппаратные "закладки" - средства слежения и несанкционированного получения информации или доступа к ней установленные в средствах связи, линиях связи, или подключённых к электросети помещения.

3. Особенности физического объекта системы информационной безопасности:

Физические параметры - наличие контролируемой зоны с установленным звук отражающим, вибрационным или нейтрализующим электромагнитные поля оборудованием;

Каналы Обмена информацией - эксплуатация кабельных или канальных сетей общего пользования или аренда частот и использование индивидуальных защищённых кабельных линий.

4. Особенности оборудование или отдельных элементов системы носителя информации:

Отдельные детали подверженные негативному воздействию электромагнитных полей: микросхемы, магнитные носители данных и т. п.;

Отдельные структурные элементы и узлы оборудования, имеющие электроакустическое или электромагнитное и техническое исполнение: телефоны, микрофоны, громкоговорители, трансформаторы, индуктивные катушки.

Случайные

К случайным уязвимым можно отнести воздействие непредвиденных факторов. Такие воздействия или очень сложно предугадать заранее. Однако они имеют определённый перечень последствий. Поэтому можно подготовиться к их оперативному устранению, что минимизирует негативные последствия или даже полностью исключит их повторение в будущем. К таким типам угроз и уязвимости можно отнести следующие:

1. Критический сбой или отказ работы системы безопасности, произошедший вследствие следующих факторов:

Выход из строя технических средств хранения, обработки и передачи информации, в том числе оборудования, которое должно осуществлять контроль доступа;

Физическое устаревание отдельных элементов, как по окончанию эксплуатационного периода, так и вследствие более интенсивного использования. Зачастую проявляется в размагничивании соответствующих носителей информации, выходу из строя отдельных микросхем из-за нарушения температурного режима, повреждение кабелей животными и т. п.;

Сбои в программном обеспечении из-за плохой совместимости или рассинхронизации различного ПО - антивирусных и сервисных программ;

Неполадки в работе или выход из строя вспомогательного или обеспечивающего оборудования - проявляется в перебоях или снижение качества электроснабжения.

2. Факторы, существенно снижающие уровень информационной безопасности:

Повреждение инженерных коммуникаций всех типов, включая водоснабжение, вентиляцию, канализацию и т. п., которые могут писать негативное воздействие на оборудование, установленное на объекте;

Неисправности в системах безопасности объекта: видеонаблюдение, охранно-пожарная сигнализация, физические повреждения ограждений и строительных конструкций здания.

Субъективные

Чаще всего, они представлены ошибочными действиями сотрудников, как на этапе разработки систем информационной безопасности, так и при их дальнейшей эксплуатации. Диагностировать данные ошибки можно с использованием следующих методик:

1. Системные ошибки, допущенные при разработке программного обеспечения, предназначенного для защиты, хранения, обработки и передачи информации. Могут возникать на следующих этапах:

Загрузка / установка программного обеспечения - ключевые ошибки алгоритмов, не предусматривающих возможность определённых действий по нарушению доступа к закрытой информации;

Использование программного обеспечения - сложный процесс работы с информацией, в том числе, касающийся её защиты от несанкционированного воздействия. Может проявляться в индивидуальных настройках сервисов, особенностях контроля информационных потоков и т. п.;

Использование аппаратуры хранения и передача данных - повреждения данных во время несанкционированного выключения аппаратных средств.

2. Нарушение доступа и компрометации в информационном поле:

Нарушение режима защиты через права доступа - как правило, связано с несанкционированным воздействием на информацию уволенных сотрудников, удалённый доступ в нерабочее время с домашних ПК и т. п.;

Нарушение режима защищённости объекта – доступ на объект, полученный не сотрудниками без должного сопровождения, что даёт возможность установки оборудования слежения;

Некорректная работа с данными - предоставление допуска сотрудникам с низкой квалификацией, которые могут некорректно выполнить поиск, изменение, сохранение и другие действия с данными, вплоть до их уничтожения.

Потенциальный ущерб от нарушений информационной безопасности

Если система управления информационной безопасностью работает некорректно, то возможно получение следующих ущерба от воздействия описанных выше угроз:

- Материальный и моральный / репутационный – физическим лицам / организации к чьей информации был получен несанкционированный доступ третьих лиц;
- Финансовый - может быть связан как с прямым хищением денежных средств, так и с затратами на восстановление информации, репутации и модернизации системы защиты информации;
- Материальный - временное ограничение доступа, сбой в работе, и невозможность выполнения основных функций из-за необходимости введения изменений в систему защиты информации.

Стоит отметить, что причинение ущерба может осуществляться двумя основными способами:

1. Совершение преступления с целью получения выгоды прямой или косвенной (преступный умысел);
2. По неосторожности - причинение вреда без злого умысла.

Оба этих способа классифицируются, как правонарушения, описанные в соответствующих разделах законодательства. Что касается специфики определение ущерба в информационном пространстве, то его причинением принято считать невыгодные последствия, связанные с материальными потерями для собственника. К примеру, это может выражаться в снижении прибыли в случае хищения конфиденциальной информации, связанной с особенностями производства уникального продукта.

Если обратиться к конкретным примерам нанесение ущерба, связанного с ошибками в управлении информационной безопасности, то наиболее распространенными являются следующие правонарушения.

"Маскарад"

Данный способ правонарушения предусматривает следующие возможности реализации:

1. Проникновение в информационную систему с использованием идентификационных данных непричастного к мошеннической системе сотрудника;
2. Предоставление заведомо ложной информации от имени другого пользователя через стандартные каналы передачи данных.

Данный способ мошенничества используется преимущественно в банковских системах для получения кредитов, манипуляций с выведением средств и т. п.

"Перехват пароля"

Несанкционированное получение данных для доступа в информационную систему путём использования специальных программ: "троянов", "червей" или

эмуляторов интерфейса окна ввода данных. Последний вариант может быть реализован. Как при помощи специального оборудования, как правило, применяется на банкоматах и других платежных терминалах, так и при помощи программного обеспечения – представляет собой сайт клон Давай информационного ресурса класса клиент-банк -> клиент.

Стоит отметить, что описанные методики являются особенно опасными, если компрометации подверглась информация точки доступа администратора. Эти пользователи имеют чрезвычайно высокий уровень возможностей работы с данными, включая возможности копирования всего массива, ее модификацию, создание новых пользователей и распределение уровней допуска т. п.

Основные направления развития системы управления информационной безопасности

Учитывая перечисленные выше угрозы информационной безопасности, особенности наносимого ими ущерба, а также основные принципы, которых необходимо придерживаться при формировании соответствующей системы, можно выделить следующие основные направления развития.

Технологическое

Использование соответствующих типов оборудования и программного обеспечения, а также формирования такой информационной структуры, которая делала бы невозможным внешняя противоправное воздействие. Кроме того, должна быть предусмотрена система не только своевременного обнаружения угрозы, но и оперативного информирования, оценки, как интенсивность его действия, так и потенциального ущерба и т. п.

Организационно-кадровое

Система управления информационной безопасности, при формировании структуры, должна опираться на квалифицированные кадры с профессиональной подготовкой и уровнем квалификации, соответствующим занимаемой должности. Что касается организационной составляющей, то здесь следует строго придерживаться правила распределения полномочий и

соответствующих им уровней допуска. Недопустимо предоставление контролирующих, администраторских и исполнительных прав одной кадровой единице.

Правовое

Немаловажным фактором системного подхода к информационной безопасности является формирование определённых правовых механизмов контроля. Это касается как государственного регулирования, так и юридического оформления соответствующих прав и обязанностей внутри организации. Правовое регулирование предполагает соблюдение следующих концепций:

1. Разработку основных принципов информационной безопасности и обеспечение системы управления и контроля соответствующими полномочиями;
2. Определение для всех субъектов системы управления информационной безопасности правового статуса, начиная от администраторов и заканчивая простыми пользователями информационной системы;
3. Необходимо предусмотреть определённые меры ответственности за несоблюдение разработанных правил, которые не выходили бы за рамки действующего законодательства.

Формирование и развитие систем управления информационной безопасности осуществляется на основе следующих факторов:

- Мониторинг информационных систем, основанный на принципах объективности и перекрёстного контроля. Осуществляется с целью качественного анализа для выявления уязвимостей и прогнозирования угроз;
- Формирование основных критериев и механизмов оценки показателей сбора, накопления и анализа соответствующей информации;
- Создание экономических правовых и организационных условий для разработки, внедрения, модернизации и развития технологий в области информационной безопасности;

- Стимулирование и контроль действий по управлению информационной безопасности.

Перечисленные выше факторы можно определить, как функции, которые выполняет постоянно действующая техническая комиссия.

3. Заключение

Как упоминалось ранее, комплексный подход является наиболее эффективным при обеспечении информационной безопасности и исключении негативного воздействия различных факторов. Однако уязвимости и вероятность их проявления могут значительно различаться в каждой информационной системе. Поэтому важной задачей управления информационной безопасностью является диагностика существующих систем, выявление наиболее вероятных уязвимостей и определение приоритетов их нейтрализации с учетом ресурсных возможностей организации.

Количественная и качественная диагностика существующих систем позволяет выявить уязвимости и разработать эффективные стратегии защиты. Это может включать обновление оборудования и программного обеспечения, улучшение организационных процессов, обучение персонала и принятие соответствующих правовых мер.

Управление информационной безопасностью является непрерывным процессом, требующим постоянного мониторинга, оценки и обновления. С учетом быстро меняющейся вредоносной среды и появления новых технологий, важно поддерживать высокий уровень готовности и адаптивности систем информационной безопасности.

Реализация эффективных мер по обеспечению информационной безопасности позволяет организациям минимизировать риски, защищать свою конфиденциальность и доверие клиентов, а также обеспечивать непрерывность бизнес-процессов и сохранение ценной информации.

Список литературы:

1. Крючков А.В., Прус Ю.В., Резниченко С.А., Технологические основы национальной информационной безопасности // Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58-63.

2. Резниченко С.А., Сиротский А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий, 2021. Том.28, №3. С. 103–117.

3. Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/

4. Сосновский М.В., Резниченко С.А. Особенности управления инцидентами ИБ в кредитно-банковской системе //Флагман науки: научный журнал. Май 2023.-СПб., Изд.ГНИИ "Нацразвитие"-2023. №4(4).

5. Резниченко С.А., Чмыхалова А.В. Анализ рисков ИБ - идентификация рисков ИБ /Особенности управления инцидентами ИБ в кредитно-банковской системе //Флагман науки: научный журнал. Май 2023.-СПб., Изд.ГНИИ "Нацразвитие"-2023. №4(4).

6. Сизов В.С., НР Резниченко С.А. Анализ программно-аппаратных средств защиты беспроводных сетей //Международный научный журнал «ВЕСТНИК НАУКИ» № 5 (62) Т.3 С. 612-624

7. Крючков А.В., Прус Ю.В., Резниченко С.А., Технологические основы национальной информационной безопасности // Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58-63.

8. Резниченко С.А., Сиротский А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий, 2021. Том.28, №3. С. 103–117.

9. Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/

10. Сосновский М.В., Резниченко С.А. Особенности управления инцидентами ИБ в кредитно-банковской системе //Флагман науки: научный журнал. Май 2023.-СПб., Изд.ГНИИ "Нацразвитие"-2023. №4(4).

11. Резниченко С.А., Чмыхалова А.В. Анализ рисков ИБ - идентификация рисков ИБ /Особенности управления инцидентами ИБ в кредитно-банковской системе //Флагман науки: научный журнал. Май 2023.-СПб., Изд.ГНИИ "Нацразвитие"-2023. №4(4).

12. Сизов В.С., НР Резниченко С.А. Анализ программно-аппаратных средств защиты беспроводных сетей //Международный научный журнал «ВЕСТНИК НАУКИ» № 5 (62) Т.3 С. 612-624