УДК: —
МРНТИ: —

[1] Толетаев Бауыржан*
[1]НУО РК
**dimash_tulkibai@mail.ru*

«УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Аннотация. В современном цифровом мире информационная безопасность стала важнейшей проблемой для организаций и мировых граждан. В этой статье исследуются существующие угрозы, возникающие проблемы информационных систем, а также их потенциальные последствия. Мы анализируем современные методы атак, включая антивирусное программное обеспечение, фишинг и утечку данных, а также рассматриваем, какие данные и ресурсы подвергаются угрозе. Статья также поднимает вопросы защиты информации и содержит советы и рекомендации по вопросам информационной безопасности. Мы рассматриваем меры реагирования и реагирования на инциденты по вопросам безопасности. В итоге, эта статья дает читателям полное представление о современных угрозах, информационной безопасности и способах защиты от них, подчеркивая эту тему в нашем цифровом обществе.

Ключевые слова: информационная безопасность, защита информации, современные угрозы.

[1] Толетаев Бауыржан
[1]НУО РК

«АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАУІП-ҚАТЕРЛЕР»

Аңдатпа. Қазіргі цифрлық әлемде ақпараттық қауіпсіздік ұйымдар мен әлем азаматтары үшін маңызды мәселеге айналды. Бұл мақалада бар қауіптер, ақпараттық жүйелердің туындайтын мәселелері, сондай-ақ олардың ықтимал салдары зерттеледі. Біз заманауи шабуыл әдістерін, соның ішінде антивирустық бағдарламалық жасақтаманы, фишингті және деректердің бұзылуын талдаймыз және қандай деректер мен ресурстарға қауіп төніп тұрғанын қарастырамыз. Мақала сонымен қатар ақпаратты қорғау мәселелерін көтереді және ақпараттық қауіпсіздік мәселелері бойынша кеңестер мен ұсыныстарды қамтиды. Біз қауіпсіздік мәселелері бойынша инциденттерге ден қою және ден қою шараларын қарастырамыз. Қорытындылай келе, бұл мақала оқырмандарға заманауи қауіптер, ақпараттық қауіпсіздік және олардан қалай қорғану керектігі туралы толық түсінік береді, бұл біздің цифрлық қоғамдағы тақырыпты көрсетеді.

Түйінді сөздер: ақпараттық қауіпсіздік, ақпаратты қорғау, заманауи қауіптер.

[1] Толетаев Бауыржан
[1]НУО РК

"INFORMATION SECURITY THREATS"

Abstract. In the modern digital world, information security has become the most important problem for organizations and global citizens. This article examines the existing threats, emerging problems of information systems, as well as their potential consequences. We analyze modern methods of attacks, including antivirus software, phishing and data leakage, and also consider which data and resources are under threat. The article also raises issues of information security and contains tips and recommendations on information security issues. We are reviewing security response and incident response measures. As a result, this article gives readers a complete picture of modern threats, information security and ways to protect against them, emphasizing this topic in our digital society.

Keywords: information security, information protection, modern threats.

«УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Б.Толетаев

Аннотация. *В современном цифровом мире информационная безопасность стала важнейшей проблемой для организаций и мировых граждан. В этой статье исследуются существующие угрозы, возникающие проблемы информационных систем, а также их потенциальные последствия. Мы анализируем современные методы атак, включая антивирусное программное обеспечение, фишинг и утечку данных, а также рассматриваем, какие данные и ресурсы подвергаются угрозе.*

Статья также поднимает вопросы защиты информации и содержит советы и рекомендации по вопросам информационной безопасности. Мы рассматриваем меры реагирования и реагирования на инциденты по вопросам безопасности.

В итоге, эта статья дает читателям полное представление о современных угрозах, информационной безопасности и способах защиты от них, подчеркивая эту тему в нашем цифровом обществе.

Ключевые слова: информационная безопасность, защита информации, современные угрозы.

Түйіндеме. *Қазіргі цифрлық әлемде ақпараттық қауіпсіздік ұйымдар мен әлем азаматтары үшін маңызды мәселеге айналды. Бұл мақалада бар қауіптер, ақпараттық жүйелердің туындайтын мәселелері, сондай-ақ олардың ықтимал салдары зерттеледі. Біз заманауи шабуыл әдістерін, соның ішінде антивирустық бағдарламалық жасақтаманы, фишингті және деректердің бұзылуын талдаймыз және қандай деректер мен ресурстарға қауіп төніп тұрғанын қарастырамыз.*

Мақала сонымен қатар ақпаратты қорғау мәселелерін көтереді және ақпараттық қауіпсіздік мәселелері бойынша кеңестер мен ұсыныстарды қамтиды. Біз қауіпсіздік мәселелері

бойынша инциденттерге ден қою және ден қою шараларын қарастырамыз.

Қорытындылай келе, бұл мақала оқырмандарға заманауи қауіптер, ақпараттық қауіпсіздік және олардан қалай қорғану керектігі туралы толық түсінік береді, бұл біздің цифрлық қоғамдағы тақырыпты көрсетеді.

Түйіндісөздер: ақпараттық қауіпсіздік, ақпаратты қорғау, заманауи қауіптер.

Abstract. *In the modern digital world, information security has become the most important problem for organizations and global citizens. This article examines the existing threats, emerging problems of information systems, as well as their potential consequences. We analyze modern methods of attacks, including antivirus software, phishing and data leakage, and also consider which data and resources are under threat.*

The article also raises issues of information security and contains tips and recommendations on information security issues. We are reviewing security response and incident response measures.

As a result, this article gives readers a complete picture of modern threats, information security and ways to protect against them, emphasizing this topic in our digital society.

Key words: information security, information protection, modern threats.

В эпоху цифрового прогресса и глобализации информационные технологии становятся непременной частью нашей повседневной жизни и деятельности. Однако, вместе с беспрецедентными возможностями, которые они предоставляют, возникают и угрозы информационной безопасности, способные оказать серьезное воздействие на наши жизни, бизнесы и даже государства.

С каждым днем растет сложность и масштаб угроз, с которыми сталкиваются организации и частные лица. От кибератак и кражи личных данных до софистицированных форм шпионажа, ландшафт информационной безопасности постоянно меняется. Важно осознавать, что угрозы не ограничиваются техническими аспектами; они проникают в

самые глубокие слои наших организаций и обществ, воздействуя на доверие, конфиденциальность и стабильность.

Начать понимание сущности угроз информационной безопасности — значит взглянуть в глаза вызовам, которые стоят перед современным цифровым миром. С этой точки зрения, давайте исследуем различные аспекты угроз информационной безопасности, их типы, источники, а также современные методы борьбы с этими вызовами.

Информационная безопасность в самом обширном смысле – это комплекс мер для защиты информации от случайного или умышленного воздействия. Вне зависимости от того, вызвано ли воздействие природными факторами или является результатом человеческой деятельности, владелец информации несет ущерб.

Принципы информационной безопасности включают:

Целостность информационных данных: гарантирует сохранение оригинального вида и структуры информации в процессе хранения и передачи, ограничивая изменения только владельцу или пользователям с легальным доступом.

Конфиденциальность: требует ограничения доступа к информационным ресурсам для определенного круга лиц. Информация становится доступной только тем пользователям, которые имеют легальные права и прошли процедуру идентификации.

Доступность информационных ресурсов: предполагает, что информация, находящаяся в открытом доступе, должна быть предоставлена полноправным пользователям своевременно и без препятствий.

Достоверность: подчеркивает принадлежность информации доверенному лицу или владельцу, являющемуся источником информации.

Обеспечение и поддержка информационной безопасности включают разнообразные меры, направленные на предотвращение, выявление и устранение несанкционированного доступа. Эти меры также защищают

информацию от повреждений, искажений, блокировок или копирования. Важно, чтобы все эти задачи выполнялись совместно для обеспечения полноценной и надежной защиты.

Основные вопросы об информационной безопасности становятся особенно актуальными, когда взлом или искажение информации могут привести к серьезным последствиям и финансовым убыткам.

Логическая цепочка трансформации информации, созданная с использованием моделирования, представляет собой следующую последовательность: УГРОЖАЮЩИЙ ИСТОЧНИК ⇒ ФАКТОР УЯЗВИМОСТИ СИСТЕМЫ ⇒ ДЕЙСТВИЕ (УГРОЗА БЕЗОПАСНОСТИ) ⇒ АТАКА ⇒ ПОСЛЕДСТВИЯ.

Угроза информации определяется как потенциальное воздействие на автоматизированную систему, приносящее ущерб потребностям других. На сегодняшний день существует более 100 видов угроз информационным системам, и важно анализировать все риски с использованием различных методик диагностики. На основе такого анализа можно эффективно построить систему защиты в информационном пространстве.

Уязвимости систем безопасности проявляются через взаимодействие с наименее защищенными частями системы. Основные уязвимости могут возникнуть из-за несовершенства программного обеспечения, аппаратной платформы, различий в характеристиках автоматизированных систем, неполноценности части процессов функционирования, неточности протоколов обмена информацией и интерфейса, а также сложных условий эксплуатации и расположения информации.

Источники угрозы чаще всего запускаются с целью получения незаконной выгоды через нанесение ущерба информации. Однако также возможны случайные действия угроз из-за недостаточной степени защиты и массового действия угрожающих факторов.

Уязвимости делятся на объективные, случайные и субъективные классы. Путем устранения или ослабления воздействия уязвимостей можно предотвратить полноценные угрозы, направленные на системы хранения информации.

Классы уязвимостей: объективные, случайные, субъективные

Объективные уязвимости напрямую зависят от технической структуры оборудования на объекте, который требует защиты, и его характеристик. Полное устранение этих факторов невозможно, однако их частичное смягчение достигается путем применения инженерно-технических методов, таких как:

Технические средства излучения:

Электромагнитные методы, включая побочные излучения и сигналы от кабельных линий и технических устройств.

Звуковые варианты, в том числе акустические сигналы или с использованием вибросигналов.

Электрические методы, такие как проскальзывание сигналов по электрическим цепям и по наводкам на линии и проводники.

Активизируемые угрозы:

Вредоносное программное обеспечение, нелегальные программы, а также технологические нарушения программ, объединенные термином "программные закладки".

Закладки аппаратуры, внедряемые напрямую в телефонные линии, электрические сети или просто в помещения.

Угрозы, создаваемые особенностями защищаемого объекта:

Расположение объекта, включая видимость, отсутствие контролируемой зоны вокруг объекта, а также наличие вибро или звукоотражающих элементов.

Организация каналов обмена информацией, такие как использование радиоканалов, аренда частот или использование общих сетей.

Угрозы, зависящие от особенностей элементов-носителей:

Детали с электроакустическими модификациями, такие как трансформаторы, телефонные устройства, микрофоны и громкоговорители, а также катушки индуктивности.

Вещи, подверженные воздействию электромагнитного поля, такие как носители, микросхемы и другие элементы.

Случайные уязвимости зависят от непредвиденных обстоятельств и особенностей окружающей информационной среды. Их практически невозможно предсказать в информационном пространстве, но важно быть готовым к их оперативному устранению. Устранение таких сбоев возможно путем проведения инженерно-технического анализа и ответных мер, принимаемых в ответ на угрозы информационной безопасности.

Сбои и отказы в работе систем:

Вследствие неисправности технических средств на разных уровнях обработки и хранения информации.

В результате неисправностей и устаревания отдельных элементов, таких как размагничивание носителей данных, кабели, соединительные линии и микросхемы.

Из-за сбоев в работе различного программного обеспечения, включая антивирусы, прикладные и сервисные программы.

Перебои в работе вспомогательного оборудования информационных систем, такие как неполадки на уровне электропередачи.

Ослабляющие факторы, влияющие на информационную безопасность:

Повреждение коммуникаций, таких как водоснабжение или электроснабжение, а также вентиляция и канализация.

Неисправности в работе ограждающих устройств, таких как заборы, перекрытия в здании, корпуса оборудования для хранения информации.

Субъективные уязвимости в большинстве случаев являются результатом неправильных действий сотрудников на уровне

разработки систем хранения и защиты информации. Их устранение возможно при помощи методик, использующих аппаратные и программные средства.

Неточности и грубые ошибки, нарушающие информационную безопасность:

На этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в процессе их использования.

В ходе управления программами и информационными системами, включая сложности обучения работе с системой, настройки сервисов и манипуляции с потоками информации.

При использовании технической аппаратуры, включая включение и выключение, эксплуатацию устройств для передачи или приема информации.

Нарушения функционирования информационных систем:

Нарушения режима защиты личных данных (проблема, связанная с уволенными сотрудниками или действующими сотрудниками в нерабочее время, которые могут получить несанкционированный доступ к системе).

Нарушения режима сохранности и защищенности (возникают при получении доступа к объекту или техническим устройствам).

Нарушения в работе технических устройств (возможны сбои в энергосбережении или обеспечении технической поддержки).

Нарушения при работе с данными (включая изменение информации, ее сохранение, поиск и уничтожение данных, а также устранение дефектов и неточностей).

Ранжирование уязвимостей Каждую уязвимость необходимо учитывать и оценивать профессионалам. Поэтому важно установить критерии оценки степени опасности угрозы и вероятности нарушения защиты информации. Эти показатели ранжируются, и среди них выделяются три основных:

Доступность: Критерий, который учитывает, насколько удобно для потенциального источника угроз использовать

конкретную уязвимость для нарушения информационной безопасности. Этот показатель включает технические параметры носителя информации, такие как размеры оборудования, его сложность, стоимость, а также возможности использования для взлома информационных систем неспециализированными средствами и устройствами.

Фатальность: Характеристика, которая оценивает глубину воздействия уязвимости на способность специалистов справиться с последствиями угрозы для информационных систем. В случае оценки только объективных уязвимостей, определяется их информативность — способность передавать полезный сигнал с конфиденциальными данными без их искажения.

Количество: Характеристика, определяющая количество элементов системы хранения и обработки информации, которым присуща любая уязвимость.

Каждый из этих показателей рассчитывается как среднее арифметическое коэффициентов отдельных уязвимостей. Формула для оценки степени опасности включает произведение коэффициентов доступности, фатальности и количества уязвимостей.

Какие источники представляют угрозу для информационной безопасности? При классификации угроз, которые обходят защиту информационной безопасности, можно выделить несколько категорий. Использование категорий является обязательным, поскольку они упрощают и систематизируют все возможные факторы. Основными параметрами являются:

Степень преднамеренности вмешательства в информационную систему:

Угроза, вызванная небрежностью персонала в информационной сфере.

Угроза, инициированная мошенниками, направленная на личную выгоду.

Характер появления угрозы:

Угроза информационной безопасности, вызванная действиями человека и представляющая искусственный характер.

Природные угрозы, неподконтрольные системам защиты и вызванные стихийными бедствиями.

Классификация непосредственной причины угрозы. Виновниками могут быть:

Человек, разглашающий конфиденциальную информацию с использованием подкупа сотрудников компании.

Природные факторы в виде катастроф или локальных бедствий.

Программное обеспечение, применение специализированных устройств или внедрение вредоносного кода, нарушающего функционирование системы.

Случайное удаление данных, санкционированные программно-аппаратные фонды, отказ в работе операционной системы.

Степень активности действия угроз на информационные ресурсы:

В момент обработки данных в информационном пространстве (действие вирусных утилит).

В момент получения новой информации.

Независимо от активности работы системы хранения информации (в случае вскрытия шифров или криптозащиты данных).

Существует также другая классификация источников угроз информационной безопасности, основанная на других параметрах, которая учитывается при анализе неисправности системы или ее взлома, учитывая несколько показателей.

Классификация угроз

Состояние источника угрозы в информационной системе может проявляться на различных уровнях, ведущих к ошибкам и сбоям при использовании ресурсов автоматизированных систем (АС). Эти состояния включают:

Внутреннюю угрозу, происходящую в самой системе, вызывающую ошибки и сбои в ресурсах АС.

Угрозу, действующую в пределах видимости АС, такую как применение подслушивающей аппаратуры, похищение распечатанных данных или кража записей с носителей данных.

Угрозу, исходящую из области действия АС, например, перехват информации в процессе передачи по каналам связи или захват акустических или электромагнитных излучений устройств.

Степень воздействия угрозы может быть активной, вносящей коррективы в структуру системы (например, использование вредоносных вирусов), или пассивной, просто крадущей информацию путем копирования без изменений в информационной системе.

Одним из важных аспектов является возможность доступа сотрудников к системе программ или ресурсов. Это может включать в себя несанкционированный доступ к системе или вред, причиняемый после согласия на доступ к ресурсам системы.

Способы доступа к основным ресурсам системы могут быть разнообразными, включая нестандартные каналы или использование стандартных каналов для открытия доступа, таких как незаконное получение паролей.

Размещение информации в системе может представлять угрозу доступа к внешним устройствам памяти, записи с видеокамер терминалов или даже незаконное проникновение в каналы связи.

Существует также классификация источников угроз на основе ранга преднамеренности, характеристик появления, непосредственной причины угрозы и степени активности действия угроз на информационные ресурсы. Учитывая эти параметры, можно более эффективно анализировать и классифицировать угрозы информационной безопасности.

Уровни и проявления ущерба могут варьироваться:

Моральный и материальный вред, причиненный физическим лицам, чья личная информация была похищена.

Финансовые потери, вызванные мошенником и связанные с расходами на восстановление информационных систем.

Затраты, связанные с материальными потерями из-за невозможности выполнения работы из-за изменений в системе защиты информации.

Моральный вред, затрагивающий деловую репутацию компании или вызывающий нарушения в мировых отношениях. Возможность причинения ущерба присутствует у лица, совершившего правонарушение (получившего несанкционированный доступ к информации или совершившего взлом системы защиты). Также ущерб может быть причинен независимо от субъекта, владеющего информацией, из-за воздействия внешних факторов (техногенных катастроф, стихийных бедствий). В первом случае вина ложится на субъекта, и определяется состав преступления, за которое выносится наказание судебным путем.

Существует два способа совершения деяния:

С умыслом (прямым или косвенным).

По неосторожности (без умышленного нанесения ущерба). Ответственность за правонарушение в отношении информационных систем определяется в соответствии с действующим законодательством страны, включая уголовное право в первом случае. Если преступление совершено по неосторожности и ущерб невелик, то рассмотрение может проводиться в рамках гражданского, административного или арбитражного права.

В заключении можно подытожить, что угрозы информационной безопасности представляют серьезное вызов для современных обществ и организаций. Развитие технологий сопровождается возрастающим разнообразием и сложностью угроз, с которыми мы сталкиваемся. От неосторожности сотрудников до продвинутых кибератак, от природных бедствий

до софистицированных хакерских методов — все эти факторы создают уязвимости, которые могут быть использованы для нарушения конфиденциальности, целостности и доступности информации.

Создание эффективной системы защиты требует не только технических решений, но и внимания к обучению персонала, разработке стратегий реагирования на инциденты и постоянному обновлению методов защиты. Важно осознавать, что угрозы постоянно эволюционируют, и поддержание актуальности защитных мер является неотъемлемой частью обеспечения информационной безопасности.

Сотрудничество между обществом, организациями и государствами также становится все более важным аспектом борьбы с угрозами информационной безопасности. Обмен знаний, опыта и ресурсов может значительно укрепить общественную стойкость и уменьшить воздействие угроз.

Защита информации — это не статичная задача, а постоянный процесс адаптации и улучшения. В борьбе с угрозами информационной безопасности ключевую роль играет осознание рисков, обучение и подготовка к переодическим изменениям в киберландшафте.

СПИСОК ЛИТЕРАТУРЫ:

1. Тершуков, Д. А. Об обеспечении международной информационной безопасности / Д. А. Тершуков // Материалы научно-практической конференции «Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства», г. Волгоград, 27–28 апреля 2017 г. – Волгоград, 2017. – С. 3–6.

2. Ханов Т.А., Жиенбеков Ж.Е. Система обеспечения информационной безопасности // Актуальные проблемы современности. 2016. №2 (12). С. 37–43.

3. Жетпісов А.Ж. О необходимости защиты информации в сфере деятельности, связанной с выявлением и раскрытием

преступлений // Актуальные проблемы современности. 2018. №3 (21). С. 68– 72.

4. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. №2 (73). С. 25–29.