Содержание:

ВВЕДЕНИЕ

Актуальность темы обусловлена тем, что государственные предприятия, частные организации и отдельные категории граждан владеют информацией, которая является ценной не только для них, но и для злоумышленников, конкурентов или зарубежных разведчиков. Неважно, в каком виде сохраняется информация и по каким каналам осуществляется ее передача, потому что на всех этапах должна функционировать организационная и инженерно-техническая защита информации.

Это не только комплекс мер, которые будут препятствовать добыче ценных данных, но и отдельная область науки. Защита информации — это право каждого субъекта и собственника бороться с методами несанкционированной утечки данных, неконтролируемого распространения сведений и вмешательства в информационные процессы организации.

Растущая информатизация экономических процессов требует повышения уровня ее безопасности. Эти вопросы обсуждаются на уровне государства. В России информационная безопасность цифровой экономики развивалась в так называемых «тепличных» условиях, когда информационная безопасность подвергала более жесткому регулированию, нежели самостоятельно развивающаяся отрасль информационных технологий.

Тем не менее, сегодняшний рынок демонстрирует довольно неплохие результаты. Сегодня российский рынок представлен десятками успешных сервис-провайдеров и фирм, специализирующихся на производстве и интеграции современных информационных технологий.

Фактически национальный рынок насыщен отечественными товаропроизводителями. В то же время распространение информационных технологий в различные отрасли экономики, будь то «умные города», он-лайн торговля или электронные госуслуги, привело к необходимости повышения технологий защиты.

Целью работы является рассмотрение видов и угроз информационной безопасности, а также проведение ситуационного анализа механизмов и

инструментов управления информационной безопасностью.

Для достижения цели необходимо решить следующие задачи:

- выявить сущность информационной безопасности фирмы;
- рассмотреть виды угроз информационной безопасности фирмы;
- провести анализ динамики инцидентов информационной безопасности;
- дать оценку основных угроз информационной безопасности
- рассмотреть методы управления информационной безопасностью в информационных системах.

Объектом исследования являются виды угроз информационной безопасности предприятия, предметом – методы снижения воздействия данных угроз.

Теоретическую основу исследования составили труды отечественных и зарубежных исследователей, монографии, материалы международных, всероссийских и региональных научно-практических конференций, материалы периодической печати и интернет-ресурсы по исследуемой проблеме.

Методологический инструментарий исследования базируется на применении общенаучных методов, таких, как: наблюдение, сравнение, анализ и синтез.

Структура работы включает в себя следующие элементы: введение, основную часть, состоящую из двух глав, заключение и список использованных источников.

1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ФИРМЫ

1.1 Сущность информационной безопасности фирмы

Для обеспечения производственной деятельности в современном мире недостаточно обладать только необходимыми материальными, денежными и трудовыми ресурсами. Развитие высоких технологий, широкое внедрение в повседневную жизнь информационных технологий требует от бизнеса адаптации своих мощностей под новые требования экономики[1].

Сейчас информация является не только источником сбора данных, так же она может выступать в качестве конечного продукта, определенного вида ценности. По сути, она выступает ключевым ресурсом современного бизнеса. Информация дает следующие возможности предпринимателю (рис. 1).

Рисунок 1 – Возможности, предоставляемые информацией[2]

Долгое время информация не рассматривалась, как экономическая категория. Только в настоящее время она стала неотъемлемой частью хозяйствующих систем.

Современный этап экономического развития базируется на огромных информационных массивах, которые требуют наличия отдельной индустрии. Любое предприятия обладает комплексом бухгалтерских, юридических, финансовых, технологических, маркетинговых и других видов данных. Умение эффективно использовать перечисленные данные составляет основу предпринимательского таланта руководителя и менеджеров среднего звена.

Стоит отметить, что предприятие действует в условиях конкурентной среды, где существуют компании, способные воздействовать на результативность итогов хозяйственной деятельности. При этом каждый экономический агент стремится к максимизации собственной выгоды, и поиска наиболее комфортных для себя условий[3].

В данном случае информация о внешней среде позволяет своевременно адаптировать особенности деятельности компании под конъюнктуру рынка. Она помогает найти пути повышения конкурентоспособности и сохранения стабильности функционирования в длительном периоде.

Оборотной стороной использования информационных технологий являются угрозы информационной безопасности. Безопасность внутренней информации влияет на сохранность данных, ноу – хау, обеспечение повышения конкурентного уровня в условиях рынка.

Информационная безопасность – довольно емкое и многогранное понятие. Его сущность претерпевает определённые изменения в зависимости от того контекста, в котором употребляется данный термин[4].

В широком смысле, на общенациональном уровне, под информационной безопасностью принято понимать определённое состояние, обеспечивающее защиту национальных интересов страны в информационном секторе, которые

определяются совокупностью трех сбалансированных элементов:

- государство;
- общество;
- личность.

На законодательном уровне информационную безопасность определяют в качестве состояния защищённости информационной среды общества, при котором она формируется, используется и развивается в интересах трех групп заинтересованных сторон, описанных выше[5].

В более узком смысле информационную безопасность принято отождествлять с защищенность информации от воздействий, способных привести к неприемлемому ущербу субъектов информационных отношений, включая владельцев и пользователей информации. Подобные воздействия могут принимать различные формы, а именно быть случайными или преднамеренными, носить естественный или искусственный характер [6].

Основными целями обеспечения информационной безопасности является защита государственной тайны, конфиденциальной информации общественного значения и личности, защита от информационного воздействия.

Информационная безопасность определяется способностью ее субъекта[7]:

- обеспечивать информационные ресурсы для поддержания своего устойчивого функционирования и развития;
- противостоять информационным угрозам, негативным воздействиям на сознание и психику людей, а также на компьютерные сети и другие технические источники информации;
- вырабатывать навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам защиты информации.

Защита информации осуществляется проведением комплекса мероприятий, направленных на обеспечение информационной безопасности. Подход к обеспечению информационной безопасности может существенно различаться для разных категорий субъектов.

Для одних на первом месте стоит секретность информации (например, государственные учреждения, банки, военные институты), для других эта секретность практически не важна (например, образовательные структуры)[8].

Субъект информационных отношений может пострадать (понести убытки или получить моральный ущерб), например, от поломки системы, которая вызовет перерыв в работе информационной системы. Примером такого проявления могут быть те же образовательные структуры, для которых сама защита от несанкционированного доступа к информации не так важна, как важна работоспособность всей системы.

Кроме того, информационная безопасность не сводится только к защите от несанкционированного доступа к информации.

1.2 Виды угроз информационной безопасности фирмы

Угрозы информационной безопасности представляют собой различные действия, которые могут привести к нарушениям информационной безопасности. Другими словами, это потенциально возможные события/процессы или действия, которые могут нанести ущерб информационным и компьютерным системам[9].

Все угрозы информационной безопасности можно разделить на два типа: естественные и искусственные.

К естественным относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д.

Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренные и непреднамеренные. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, которые не входят в число необходимых для работы, в дальнейшем нарушающих работу системы, что и приводит к потере информации.

Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат этого вида угроз – огромные потери компанией денежных средств и интеллектуальной собственности.

Самым слабым звеном в обеспечении информационной безопасности чаще всего оказывается человек. На рисунке 2 представлены основные виды угроз информационной безопасности.

Рисунок 2 – Виды угроз информационной безопасности[10]

Представленные выше факторы, несущие в себе угрозу безопасности информационной среды, принято называть информационными угрозами.

Источник угроз может иметь разное положение. В зависимости от этого фактора также выделяют три группы[11]:

- угрозы, источник которых находятся вне контролируемой группы компьютерной системы (пример – перехват данных, передаваемых по каналам связи);

- угрозы, источник которых – в пределах контролируемой зоны системы (это может быть хищение носителей информации);

- угрозы, находящиеся непосредственно в самой системе (например, некорректное использование ресурсов).

В зависимости от различных способов классификации все возможные виды угрозы информационной безопасности в деятельности современного предприятия можно разделить на следующие основные подгруппы:

- нежелательный контент;
- несанкционированный доступ;
- утечки информации;
- потеря данных;
- мошенничество;
- кибервойны;
- кибертерроризм.

Нежелательный контент включает в себя не только вредоносные программы, потенциально опасные программы и спам, которые непосредственно созданы для того, чтобы уничтожить или украсть информацию, но и сайты, которые запрещены законодательством, или нежелательные сайты, что содержат информацию, не соответствующую возрасту потребителя.

Несанкционированный доступ – просмотр информации сотрудником, который не имеет разрешения пользоваться данной информацией, путем нарушения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, какая информация и где она хранится, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных

программ.

Утечка информации в зависимости от того, чем она была вызвана, может разделяться на умышленную и случайную. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и человека. А умышленные, в отличие от случайных, организовываются преднамеренно, с целью получить доступ к данным, нанести ущерб[12].

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действия пользователей, будь то они сотрудниками или злоумышленниками.

Не менее опасной угрозой является фрод (мошенничество с использованием информационных технологий). К мошенничеству можно отнести не только манипуляции с кредитными картами (кардинг) и взлом онлайн-банка, но и внутренний фрод. Целью этих экономических преступлений является обход законодательства, политики, нормативных актов компании, присвоение имущества.

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на АСУ ТП различных предприятий[13].

Но подобные атаки не проводятся без предварительной разведки, для чего и нужен кибершпионаж, который поможет собрать необходимые данные. Существует также такое понятие, как информационная война, которая отличается от обычной войны только тем, что в качестве оружия выступает тщательно подготовленная информация.

Наиболее полная классификация угроз информационной безопасности представлена в приложении 1.

Так или иначе, информационная безопасность непосредственно связана с необходимостью защиты информационной среды, от внутренних и внешних угроз. Иначе говоря, она предполагает необходимость обеспечения целостности и устойчивости функционирования информационных систем.

Немаловажным вопросом в обеспечении информационной безопасности является приемлемость ущерба. Это значит, что стоимость средств защиты и необходимых

мероприятий не должны превышать размер ожидаемого ущерба, иначе это будет экономически нецелесообразным. Т.е. с каким-то возможным ущербом придется смириться (т.к. от всех возможных ущербов защититься невозможно), а защищаться необходимо от того, с чем смириться является невозможным.

Например, чаще всего недопустимым ущербом информационной безопасности является материальные потери, а целью защиты информации должно быть уменьшение размеров ущерба до допустимых значений.

Таким образом, можно отметить, что вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям.

Задача обеспечения информационной безопасности в свою очередь подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации.

2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРЕДОТВРАЩЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

2.1 Анализ динамики инцидентов информационной безопасности

Ежегодно раз в полгода Центр мониторинга по информационной безопасности публикует отчеты, в которых ведется аналитика зафиксированных событий и инцидентов информационной безопасности.

В период с 1 января по 30 июня 2018 года сотрудники Центра мониторинга контролировали информационные системы организаций с общим числом подключённых узлов около 28 200 (рабочие места, веб, почта, файловые хранилища и т. д.).

Рисунок 3 – Количество зафиксированных событий ЦИБ в динамике[14]

За шесть месяцев 2018 года сенсоры зафиксировали 112 млн. событий информационной безопасности. Как видно, наибольший объем событий был зафиксирован в первом полугодии 2017 г., пик которых пришелся на март 2017 г. В период с 1 января по 31 марта 2017 года сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 12 000 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

За три месяца сенсоры зафиксировали и проанализировали 137 873 416 событий информационной безопасности и выявили 98 инцидентов.

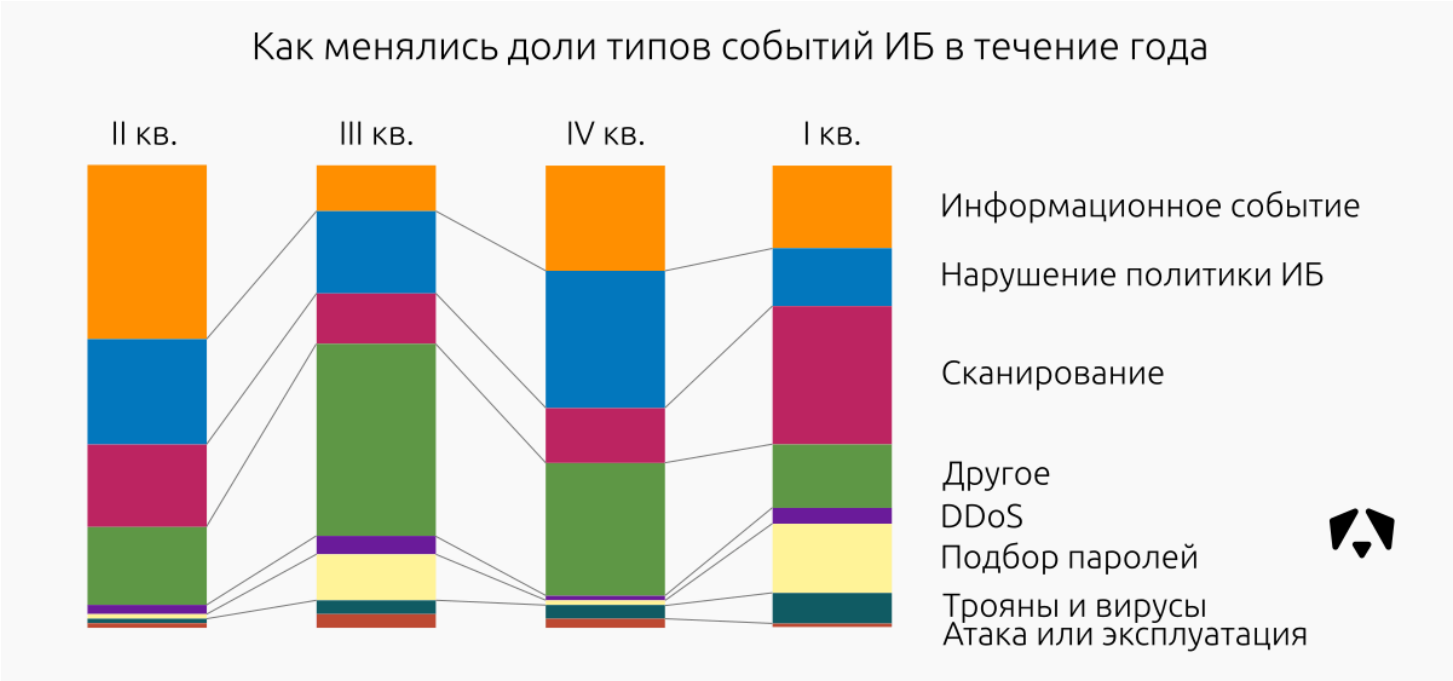

Рисунок 4 – Доли зафиксированных событий в 2016-2017 гг.[15]

Самое значимое изменение по сравнению с предыдущим периодом — рост доли событий, связанных со сканированием информационных ресурсов и попытками подбора паролей к различным информационным системам. Также немного увеличилась активность вредоносного ПО.

Со 2 полугодия 2017 г. наблюдается снижение количества зарегистрированных событий информационной безопасности с учётом увеличения количества контролируемых ресурсов и инцидентов, что обусловлено следующими факторами [16]:

- были оптимизированы некоторые правила базы AM Rules. Благодаря этому множество одинаковых событий агрегируются.
- в настоящее время Центр мониторинга быстрее реагирует на DDoS-атаки и другие инциденты информационной безопасности, проявляющиеся в большом количестве срабатываний сигнатур, и помогает предотвращать их развитие на ранней стадии.

Всего за шесть месяцев 2018 г. было зарегистрировано 434 инцидента.

Рисунок 5 – Динамика инцидентов в 2016-2018 гг.[17]

Как видно, всплеск динамики инцидентов приходится также на 1 п. 2017 г., темп прироста составил 227,03%, к 1 п. 2018 г. темп прироста снизился до 19,56%.

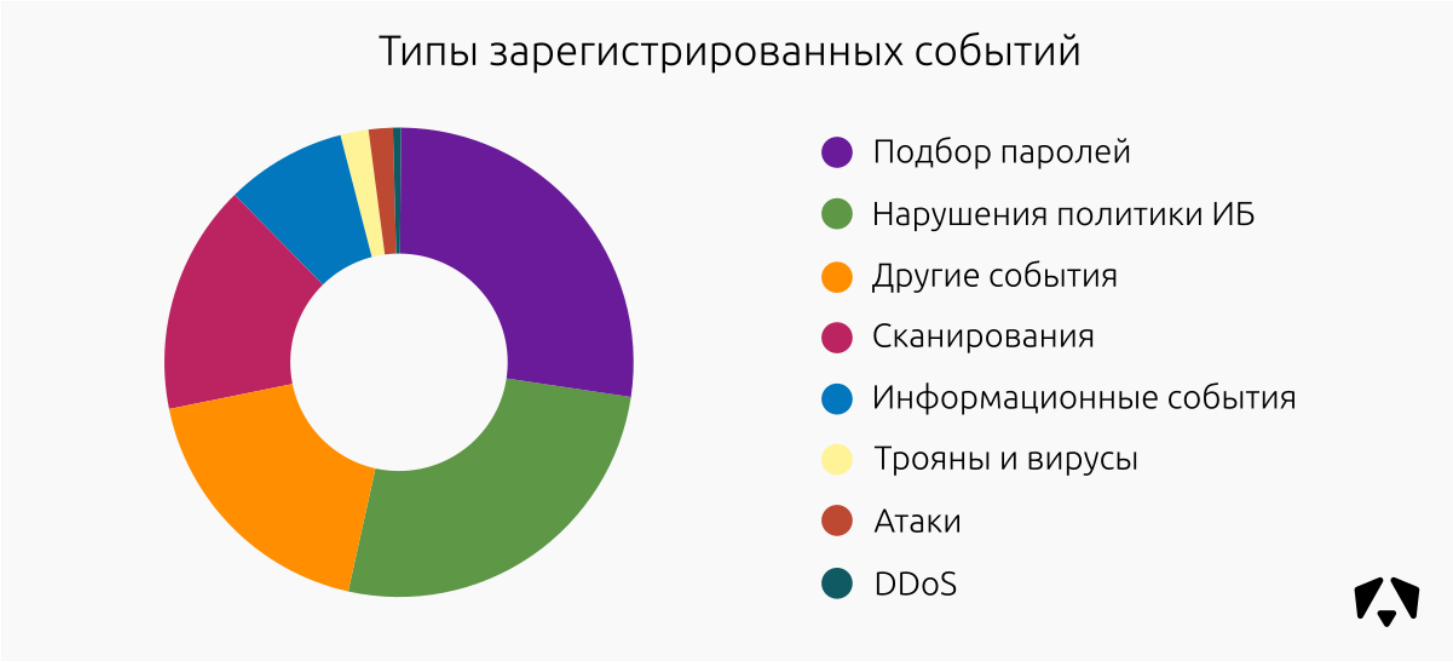

Рисунок 6 – Типы зарегистрированных событий в 2018 г.[18]

Большая доля зарегистрированных событий приходится на «Подбор паролей» - 42%, сканирование занимает 24% (41 646 524 зафиксированных события). На нарушение политики безопасности приходится 29%.

В отчете указано, что распределение зафиксированных событий по типам не сильно изменилось по сравнению со второй половиной 2017 года. Самое заметное изменение — выход на первое место попыток подбора паролей к различным сервисам.

Нарушения политик, сканирования и информационные события всё так же остаются в «топе». Увеличилось количество событий в категории «Сканирование».

Среди выявленных 434 инцидентов можно выделить классы, представленные в таблице 1.

Таблица 1 - Классы выявленных инцидентов в 2018 г.[19]

Класс инцидента	Низкая критичность	Средняя критичность	Высокая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	3	75	101	179	41%
Атаки и попытки эксплуатации уязвимостей	4	68	57	129	30%
Подбор паролей	2	27	35	64	15%
Нарушение политики ИБ	6	32	6	44	10%
DDoS	3	5	10	18	4%

Наиболее актуальными и критичными из выявленных являются атаки, связанные с попытками получения несанкционированного доступа к ресурсам организаций.

В таблице 2 представлена динамика инцидентов со второго полугодия 2016 г. по второе полугодие 2018 гг.

Таблица 2 - Динамика доли выявленных инцидентов в 2018 г

Класс инцидента	IIкв. 2016	IIIкв. 2016	IVкв. 2016	Iкв. 2017	I кв. 2018 г.
Вредоносное ПО	43,5	42,8	51	52	41
DDoS	8,7	14,3	1,9	3	4
Нарушение политики ИБ	30,4	14,3	13,2	9	10
Подбор паролей	17,4	23,8	13,2	14	15
Атака и эксплуатация уязвимостей		4,8	20,7	22	30

Из таблицы видно, что в исследуемом периоде наблюдается снижение попыток получения информации путем внедрения вредоносного ПО – с 43,5% до 41% (при этом в 1 квартале 2017 г. зафиксирован максимум – 52% по данной статье), со 2 квартала 2016 г. значительно снизились инциденты, связанные с нарушением политики информационной безопасности – снижение составило 20,4% - с 30,4% до 10%.

Таким образом, можно отметить, что снижение числа инцидентов нарушения информационной безопасности связано прежде всего с повышением качества борьбы с основными угрозами, однако, с каждым днем появляются все новые угрозы, которые направлены на поиск уязвимостей, в 2018 г. их доля увеличилась до 30%.

2.2 Оценка основных угроз информационной безопасности

Для качественной оценки основных угроз информационной безопасности составим таблицу 3, в которой представим наиболее часто используемые техники воздействия на системы, повлёкшие инцидент информационной безопасности.

Таблица 3 – Угрозы ИБ и техника воздействия

Угроза	Техника воздействия
Рекламное ПО	Заражение конечной системы, передача на командный сервер информации о пользователе, показ таргетированной рекламы.
Перебор паролей	Попытки подбора аутентификационной информации для доступа к сервисам и ресурсам контролируемых организаций — RDP, SSH, SMB, DB, Web.

Продолжение таблицы 3

Нарушение политик ИБ	Нарушение пользователями/администраторами контролируемых ресурсов требований политик ИБ в части использования устаревших версий или недоверенного ПО. Данное ПО может быть использовано злоумышленником для атаки путём эксплуатации уязвимости. Также использование ресурсов компании для получения собственной выгоды (майнинг bitcoin/ethereum). Использование торрент-трекеров.
Вирусное ПО	Заражение конечной системы, распространение вируса по локальной сети, отключение/блокировка служб, препятствующих распространению вируса, попытки проведения иных атак внутри сети для получения критичной информации и передачи на командные серверы.
DDoS с использованием ресурсов организации	DDoS Amplification — техника подмены своего адреса на адрес жертвы и генерации запросов небольшого размера к открытым сервисам. На запрос сервис возвращает ответ в несколько десятков раз большего объема на адрес «отправителя». Используя большое количество ресурсов различных организаций, злоумышленник осуществляет DDoS-атаку на жертву.

Попытки эксплуатации уязвимостей	Использование недостатков в системе для нарушения целостности и нарушения правильной работы системы. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадёжных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.
Deface WEB-ресурсов	Хакерская атака, при которой страницы и важная информация заменяются на другие, как правило вызывающего вида (реклама, предупреждение, угроза, пропаганда) Зачастую, доступ ко всему остальному сайту блокируется, или же прежнее содержимое удаляется.

На рисунке 7 представлены данные по критичности инцидентов 2018 г.

Рисунок 7 – Оценка критичности зафиксированных инцидентов в 2018 г.

По самому большому классу — вредоносное ПО в 2018 г. наблюдаются следующие тенденции:

- как и во втором квартале 2017 года продолжаются заражения семейством вредоносов WannaCry и Petya/notPetya. Несмотря на всеобщее освещение этой проблемы, всё равно остаётся очень много уязвимых узлов;
- большинство найденных вредоносных файлов представляют собой ПО для майнинга криптовалют. Хакеры стали немного «добрее» и пытаются заработать на ресурсах пользователей.
- также часто обнаруживаются рекламное потенциально-нежелательное ПО. В основном пользователи скачивают его вместе с взломанными или бесплатными программами и при установке ПО для быстрого поиска драйверов, например, DriverPack и аналоги.

Что касается «Эксплуатации уязвимостей», то наблюдается большое количество попыток эксплуатации уязвимостей в Apache Struts, Drupalgeddon, и EternalBlue. Несмотря на то, что загрузка шифровальщиков через данную уязвимость уже минимальна, её активно используют для распространения другого вредоносного ПО. И если зашифрованные данные видны сразу, то активность другого вредоносного ПО обычный пользователь может даже и не заметить. Остальную массу заведённых инцидентов в категории составляют попытки эксплуатации XSS, внедрение PHP- и SQL-инъекций.

Как показывают результаты анализа, сотрудники часто используют корпоративные ресурсы в своих личных целях: от распечатки доклада ребёнку в школу до доступа в личный интернет-банк. Сейчас же эксперты столкнулись с тем, что сотрудники майнят bitcoin и ethereum на вычислительных ресурсах организации. Такие инциденты также попали в «Нарушение политики»[20].

Большая часть инцидентов приходится на начало недели. Связаны они, в первую очередь, с активностью вредоносного программного обеспечения на рабочих местах сотрудников.

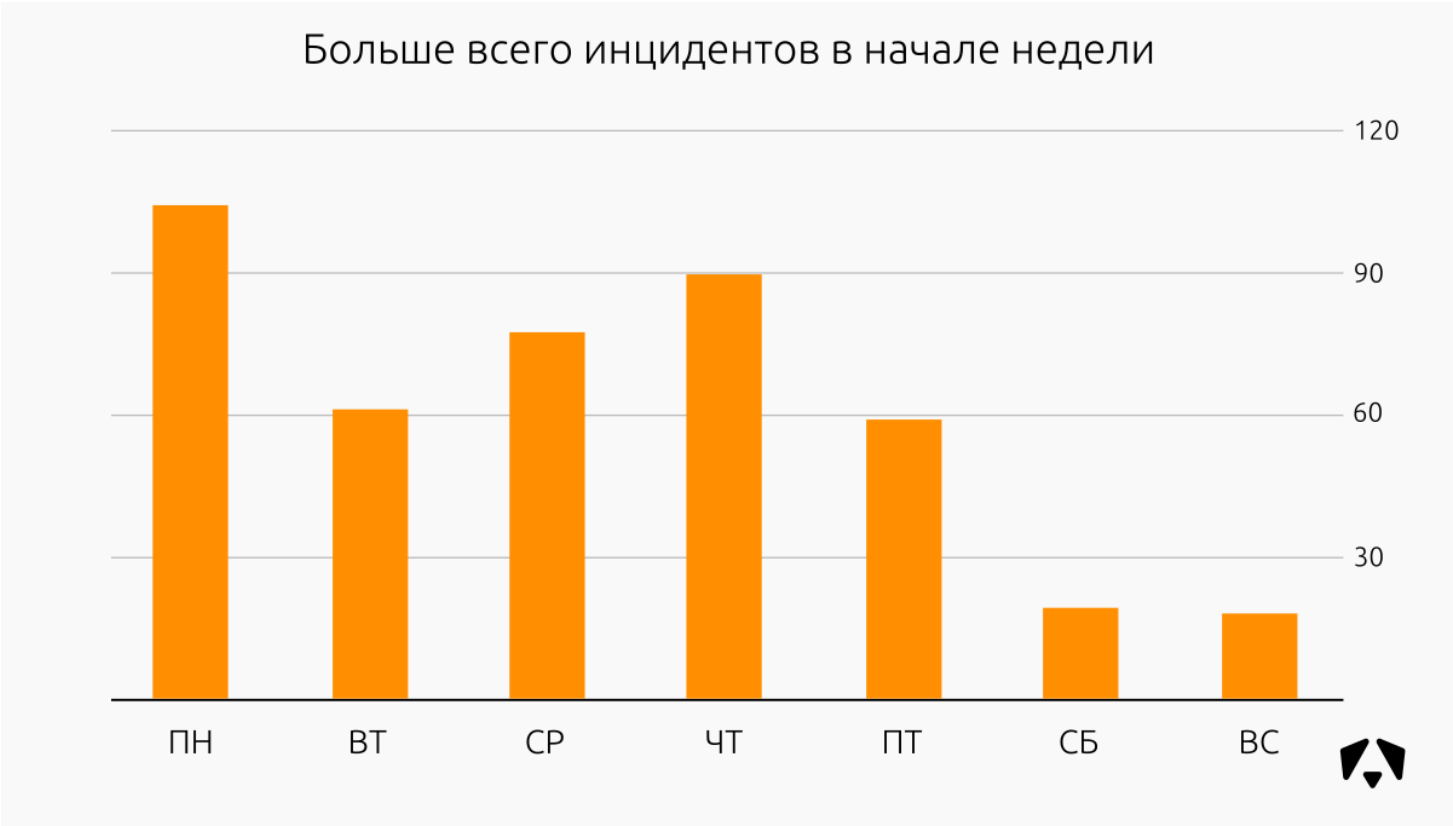

Рисунок 8 – Активность угроз информационной безопасности по дням недели[21]

Серьёзных негативных последствий для контролируемых информационных систем такие инциденты не несут, но администраторы тратят время на антивирусные проверки, а пользователи в это время не могут полноценно работать.

2.3 Методы управления информационной безопасностью в информационных системах

Для обеспечения безопасности информации в информационных системах могут быть использованы следующие методы[22]:

- препятствие;
- управление доступом;
- методы криптографии;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Препятствие – физическое преграждение пути к защищаемой информации (к техническому оборудованию, носителям информации и т.д.).

Управление доступом – методы защиты информации через регулирование использования ресурсов информационных технологий и информационной системы. Управление доступом должно препятствовать абсолютно всем возможным путям несанкционированного доступа к защищаемой информации.

Защита информации с помощью управления доступом происходит через[23]:

- идентификацию пользователей и персонала (присвоение персонального идентификатора);
- опознание объекта по идентификатору;
- проверку полномочий доступа к информации или объекту;
- регистрацию обращений к информации;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Криптографические методы защиты – шифрование информации. Методы шифрования широко применяются при обработке и хранении информации.

Защиту от атак вредоносных программ призван обеспечить комплекс различных методов организационного характера и использование антивирусных программ, результатом чего является снижение вероятности заражения ИС, определение фактов инфицирования системы, снижение или предотвращение последствий информационных заражений, уничтожение вирусов, последующее восстановление информации.

Регламентация – ограничение времени работы, ограниченный доступ людей к информации, ограничение доступа по определенным дням, времени суток, часам и т.п. Создание таких условий работы с защищаемой информацией нормы и стандарты по защите будут выполняются в наибольшей степени.

Принуждение – метод защиты информации, при котором пользователи и персонал ИС соблюдают правила работы с защищаемой информацией под угрозой ответственности (материальной, административной или уголовной).

Побуждение – метод, который побуждает (за счет соблюдения уже сложившихся морально-этических норм) субъектов ИС не нарушать установленные порядки.

Технические средства защиты информации делятся на аппаратные и физические. К физическим средствам относят инженерные устройства и сооружения, которые препятствуют физическому проникновению на объекты защиты и осуществляют защиту персонала, материальных, информационных и других ценностей (например, решетки, замки, сейфы, сигнализация и т.п.)[24].

Организационные средства обеспечивают мероприятия, которые делают невозможными или затрудняют разглашение, утечку, несанкционированный доступ к информации на нормативно-правовой основе.

Законодательные средства защиты регламентируют правила работы с информацией и устанавливают порядок ответственности за их нарушение. Законодательные средства защиты определяются законодательными актами страны.

Морально-этические средства защиты включают нормы поведения, которые могут быть неписанными (например, честность) или оформленными в виде правил и предписаний.

Как правило, они не утверждены законодательством, но считаются обязательными для исполнения. Примером таких правил может быть свод этических правил общения в сети и т.п.

Основные инструменты обеспечения информационной безопасности цифровой экономики представлены на рисунке 9.

Рисунок 9 - Инструменты обеспечения информационной безопасности[25]

Одним из наиболее ярких примеров обеспечения информационной безопасности в экономической сфере выступает развитие биометрических технологий защиты, когда касанием пальца идентифицируется и подтверждается личность человека. Наибольшее распространение подобные технологии получают в банковской сфере – уже сегодня оплатить покупки с карты можно в одно касание пальца на смартфоне. В ближайшие годы банковская отрасль планирует разработать и внедрить систему кредитования, в основе которой будет лежать распознавание личности клиента по голосу.

Все его данные, включая кредитную историю, будут занесены в единую базу данных. Также одним из наиболее распространенных в современной бизнес-практике инструментов выступает использование электронных цифровых

подписей, содержащих в себе определённый цифровой код.

Подобные технологии активно используются в системе государственных закупок и электронных торгов, а также при сдаче отчетности в контролирующие органы.

Таким образом, можно отметить, что наблюдается значительное увеличение роста таких угроз как вредоносное ПО, подбор паролей и атаки, что свидетельствует о необходимости более активного использования таких методов как управление доступом, методы криптографии, противодействие атакам вредоносных программ, регламентация.

Можно отметить, что обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасных программ на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий. А в борьбе с мошенничеством следует использовать анти-фрод системы, которые предоставляют возможность мониторить, обнаруживать и управлять уровнем фрода.

ЗАКЛЮЧЕНИЕ

В широком смысле, на общенациональном уровне, под информационной безопасностью принято понимать определённое состояние, обеспечивающее защиту национальных интересов страны в информационном секторе.

Угрозы информационной безопасности представляют собой различные действия, которые могут привести к нарушениям информационной безопасности. Другими словами, это потенциально возможные события/процессы или действия, которые могут нанести ущерб информационным и компьютерным системам

Нарушение информационной безопасности может быть вызвано как спланированными действиями злоумышленника, так и неопытностью сотрудника. Пользователь должен иметь хоть какое-то понятие об ИБ, вредоносном

программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе.

Чтобы пробиться через защиту и получить доступ к нужной информации злоумышленники используют слабые места и ошибки в работе программного обеспечения, веб-приложений, ошибки в конфигурациях файрволов, прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов.

Вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям.

Задача обеспечения информационной безопасности в свою очередь подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации.

За шесть месяцев 2018 года сенсоры зафиксировали 112 млн. событий информационной безопасности. Наибольший объем событий был зафиксирован в первом полугодии 2017 г., пик которых пришелся на март 2017 г.

Большая доля зарегистрированных событий приходится на «Подбор паролей» - 42%, сканирование занимает 24% (41 646 524 зафиксированных события). На нарушение политики безопасности приходится 29%. Распределение зафиксированных событий по типам не сильно изменилось по сравнению со второй половины 2017 года. Самое заметное изменение — выход на первое место попыток подбора паролей к различным сервисам.

Нарушения политик, сканирования и информационные события всё так же остаются в «топе». Увеличилось количество событий в категории «Сканирование».

Большая часть инцидентов приходится на начало недели. Связаны они, в первую очередь, с активностью вредоносного программного обеспечения на рабочих местах сотрудников.

На наш взгляд, обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную

установку потенциально опасных программ на компьютер.

Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) // Система Консультант Плюс
2. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (в ред. от 04.08.2018 года)// Собрание законодательства Российской Федерации, 1994, № 32, ст. 773; 2018, № 32, ст. 5132.
3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция) // Система Консультант Плюс
4. ГОСТ Р 57580.2-2018. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия" (утв. и введен в действие Приказом Росстандарта от 28.03.2018 N 156-ст) // Система Консультант Плюс
5. Васильков А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. — М.: Форум, 2018. — 528 с.
6. Занько, Н.Г. Безопасность жизнедеятельности / Н.Г. Занько, К.Р. Малаян и др. - СПб.: Лань, 2016. - 696 с.
7. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М.: ФОРУМ: ИНФРА-М, 2018. — 432 с.
8. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.
9. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2018. — 416 с

10. Основные положения информационной безопасности: учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. — М.: ФОРУМ: ИНФРА-М, 2018. — 208 с.
11. Управление информационными рисками. Экономически оправданная безопасность: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.: ДМК Пресс, 2018. - 396 с.
12. Шестакова, Л. В. Информатика и информационно-коммуникационные технологии. — М.: Бином, 2017. — 176 с.
13. Александрова М. Ю. Правовое регулирование информационной безопасности образовательной организации // Молодой ученый. — 2018. — №7. — С. 123-124.
14. Буянов Д. С. Информационная безопасность в социальных сетях // Молодой ученый. — 2018. — №39. — С. 14-16.
15. Есипова А. А., Ребко Э. М. Основные структурные компоненты культуры безопасности жизнедеятельности // Молодой ученый. — 2014. — №18.1. — С. 36-38.
16. Калужин Е. А., Монастырский Д. С. Особенности обеспечения информационной безопасности электронного документооборота территориально распределенного предприятия // Молодой ученый. — 2017. — №3. — С. 32-35.
17. Мухамадиева З. Б. Защита информации в информационных системах // Молодой ученый. — 2018. — №9. — С. 34-36.
18. Стромова Н. С. Информационная безопасность, кодирование и декодирование данных // Молодой ученый. — 2018. — №39. — С. 16-20.
19. Титов В.А., Замараева О.А., Кузин Д.О. Мероприятия по организации инженерно-технической защиты информации // Фундаментальные исследования. – 2014. – № 5-3. – С. 573-576
20. Виды угроз информационной безопасности // Режим доступа https://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html
21. Отчёт Центра мониторинга информационной безопасности за I квартал 2017 года https://habrahabr.ru/company/pm/blog/326810/
22. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/
23. Угрозы информационной безопасности //Режим доступа: https://www.anti-malware.ru/threats/information-security-threats

ПРИЛОЖЕНИЕ

По характеру нарушения	• нарушение конфиденциальности данных • нарушение работоспособности ЭВМ • незаконное вмешательство в функционирование ЭВМ и т.д.
По тяжести нарушения	• незначительные ошибки • мелкое хулиганство • серьезные преступления/природные и техногенные катастрофы
По предвидению последствий нарушителем	• намеренные нарушения • ненамеренные нарушения
По мотивации	• злонамеренные нарушения • незлонамеренные нарушения
По месту возникновения	• внешние угрозы • внутренние угрозы (угрозы со стороны инсайдеров)
По законченности	• реализованные • нереализованные
По объекту воздействия	• угрозы, нацеленные на всю информационную систему • угрозы, нацеленные на отдельные компоненты ИС
По причине возникновения	• угрозы, возникшие из-за недостаточности средств технической защиты • угрозы, возникшие из-за недостаточности организационных мер
По каналу проникновения	• угрозы, проникающие через уязвимости ПО, бесконтрольные съёмные носители • угрозы, проникающие через бреши в системах авторизации, недостатки систем хранения документов и т.д.
По виду реализации угрозы	• вредоносные программы, спам-письма, программные закладки, хакерские атаки • уязвимые процедуры авторизации и другие регламенты ИБ • стихийные бедствия
По происхождению	• антропогенные • техногенные • природные
По размеру ущерба	• незначительные • значительные • критичные

Виды угроз информационной безопасности

1. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. ↑

2. Угрозы информационной безопасности //Режим доступа: https://www.anti-malware.ru/threats/information-security-threats ↑

3. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. — 416 с. ↑

4. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. ↑

5. Александрова М. Ю. Правовое регулирование информационной безопасности образовательной организации // Молодой ученый. — 2018. — №7. — С. 123-124. ↑

6. Васильков А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. — М.: Форум, 2018. — 528 с. ↑

7. Калужин Е. А., Монастырский Д. С. Особенности обеспечения информационной безопасности электронного документооборота территориально распределенного предприятия // Молодой ученый. — 2017. — №3. — С. 32-35. ↑

8. Управление информационными рисками. Экономически оправданная безопасность: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.: ДМК Пресс, 2018. - 396 с. ↑

9. Шестакова, Л. В. Информатика и информационно-коммуникационные технологии. — М.: Бином, 2017. — 176 с. ↑

10. Виды угроз информационной безопасности // Режим доступа https://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html ↑

11. Стромова Н. С. Информационная безопасность, кодирование и декодирование данных // Молодой ученый. — 2018. — №39. — С. 16-20. ↑

12. Мухамадиева З. Б. Защита информации в информационных системах // Молодой ученый. — 2018. — №9. — С. 34-36. ↑

13. Основные положения информационной безопасности : учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. — М. : ФОРУМ : ИНФРА-М, 2018. — 208 с. ↑

14. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

15. Отчёт Центра мониторинга информационной безопасности за I квартал 2017 года https://habrahabr.ru/company/pm/blog/326810/ ↑

16. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

17. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

18. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

19. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

20. Отчёт Центра мониторинга информационной безопасности за I квартал 2017 года https://habrahabr.ru/company/pm/blog/326810/ ↑

21. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года // Блог компании Перспективный мониторинг https://habr.com/ru/company/pm/blog/424475/ ↑

22. Есипова А. А., Ребко Э. М. Основные структурные компоненты культуры безопасности жизнедеятельности // Молодой ученый. — 2014. — №18.1. — С. 36-38. ↑

23. Занько, Н.Г. Безопасность жизнедеятельности / Н.Г. Занько, К.Р. Малаян и др. - СПб.: Лань, 2016. - 696 с. ↑

24. Титов В.А., Замараева О.А., Кузин Д.О. Мероприятия по организации инженерно-технической защиты информации // Фундаментальные исследования. – 2014. – № 5-3. – С. 573-576 ↑

25. Буянов Д. С. Информационная безопасность в социальных сетях // Молодой ученый. — 2018. — №39. — С. 14-16. ↑