УДК 004.056

Ямин Артём Дмитриевич,
студент магистратуры,
Школа управления и междисциплинарных исследований,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург, Российская Федерация

Тарасьев Александр Александрович,
кандидат экономических наук, доцент,
кафедра анализа систем и принятия решений,
Высшая школа экономики и менеджмента,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург, Российская Федерация

МЕХАНИЗМЫ И ПРИНЦИПЫ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ

Аннотация:
Статья описывает деятельность государства и предприятий в области информационной безопасности, а также общий обзор структуры системы обеспечения информационной безопасности.
В качестве описания соответствия применяемых мер защиты представлена классификация организационных и технических мер защиты.

Ключевые слова:
Информационная безопасность, система обеспечения информационной безопасности, кибератака, киберпреступность, значимый объект критической информационной инфраструктуры.

На данный момент экономика современных предприятий все больше зависит от актуальности внедренных им систем информационной защиты. Основной предпосылкой для развития информационной безопасности (ИБ) в РФ стали санкции, внешняя и внутренняя политика государства, согласно которым внедрение и развитие систем обеспечения ИБ (СОИБ) на предприятиях РФ, относящихся к субъектам критической информационной инфраструктуры (КИИ) страны, стали необходимостью.

Основными принципами СОИБ является обеспечение конфиденциальности, целостности и доступности информации. Внедрение СОИБ на предприятиях позволяет гарантировать обеспечение надлежащего уровня безопасности корпоративных данных, активов и информации на разных этапах бизнес-процессов.

Защита значимых объектов КИИ (ЗОКИИ) играет важную роль как для сохранения суверенности государства, так и для обеспечения безопасности общества и предприятий.

К числу основных задач СОИБ ЗОКИИ относятся:

1. Недопущение неправомерного доступа к информации, обрабатываемой ЗОКИИ, ее уничтожения, модифицирования, блокирования, копирования, распространения и т.д.
2. Предотвращение воздействия на технические средства обработки информации.
3. Восстановление функционирования ЗОКИИ.
4. Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и национальным координационным центром по компьютерным инцидентам (НКЦКИ) [1].

Для решения вышеперечисленных задач государство осуществляет следующие мероприятия:

- регулирование законов в сфере ИБ;
- реализация государственного контроля за соблюдением мер ИБ;
- введение политики импортозамещения средств защиты информации (СрЗИ);
- усовершенствование методики моделирования угроз ИБ;
- постоянное пополнение банка данных угроз безопасности информации.

За 2022 год было принято 257 нормативных правовых актов, относительно регулирования сфер ИБ, ИТ и цифровой экономики. Большая часть нововведений коснулась сферы цифровой экономики, нормативная база которой менялась более чем в половине случаев (51,8%). Заметные доли получили безопасность КИИ (5,8%) и импортозамещение – 4,7% [2].

Предприятия, заинтересованные в соблюдении требований ИБ и защите своих активов от кибератак, проводят мероприятия по развитию ИБ, а также внедряют меры защиты, минимизирующие возможность несанкционированного доступа к информации.

В числе таких мер:

- проведение аудитов безопасности информации;
- определение категорий ЗОКИИ;
- разработка и применение организационно-распорядительных документов (ОРД) в сфере ИБ;
- разработка модели угроз ИБ и модели нарушителя для ЗОКИИ;
- проектирование и внедрение СОИБ;
- информирование и обучение персонала реагированию на прецеденты в сфере ИБ;
- постоянное взаимодействие с ГосСОПКА и НКЦКИ.

В зависимости от объекта защиты СОИБ может состоять из различных подсистем, каждая из которых включает в себя организационные и технические мероприятия. Примерами таких подсистем являются:

- подсистема управления доступом;
- подсистема регистрации и учета событий ИБ;
- подсистема защиты от вредоносного программного обеспечения;
- подсистема обеспечения целостности;
- подсистема контроля защищенности;
- подсистема сетевой безопасности;
- подсистема обеспечения непрерывности функционирования;
- подсистема управления СрЗИ.

Помимо встроенных механизмов защиты информации операционных систем (ОС), активного сетевого оборудования, периферийного оборудования и т.д. активно применяются наложенные СрЗИ. К их числу относятся средства антивирусной защиты, средства резервного копирования и восстановления данных, средства контроля целостности системы, средства криптографической защиты информации, средства защиты от несанкционированного доступа (НСД), различные SIEM-системы и т.д.

В ЗОКИИ в зависимости от их категории значимости и угроз ИБ должны быть реализованы следующие организационные и технические меры:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты ИБ (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО) [3].

В качестве примера в таблице 1 приведены мероприятия по защите информации для меры «Идентификация и аутентификация (ИАФ)» в зависимости от категории значимости ЗОКИИ.

Таблица 1 – Меры безопасности и меры защиты

Мера безопасности	**Категория**			**Меры защиты**
	III	**II**	**I**	
Идентификация и аутентификация (ИАФ)				
ИАФ.0 Регламентация правил и процедур идентификации и аутентификации	+	+	+	Политика идентификации и аутентификации или раздел Политики ИБ
ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	1.Учетные данные домена/ОС; 2.Учетные данные специального программного обеспечения (СПО); 3.УЗ, созданные с помощью СрЗИ
ИАФ.2 Идентификация и аутентификация устройств	+	+	+	1.Определен перечень устройств/типов устройств, подлежащих идентификации; 2.С помощью встроеных механизмов ОС 3.С помощью механизма учета устройств СрЗИ

Мера безопасности	Категория			Меры защиты
	III	II	I	
ИАФ.3 Управление идентификаторами	+	+	+	1.Процедуры должны быть описаны в ОРД; 2.С помощью контроллера домена; 3.С помощью средств ОС/СПО; 4.С помощью СрЗИ
ИАФ.4 Управление средствами аутентификации				
ИАФ.5 Идентификация и аутентификация внешних пользователей				
ИАФ.6 Двусторонняя аутентификация	-	-	-	Применяется как дополнительная мера. С помощью применения SSL – сертификата, с целью подтверждения обращающейся и принимающей сторон
ИАФ.7 Защита аутентификационной информации при передаче	+	+	+	1.Информация не передается в смежные системы; 2.Запароленный архив/файл. Пароль передается другим способом связи (по телефону, лично в руки и т.д.)

Таким образом, чем быстрее происходит цифровизация общества, тем острее стоит проблема ИБ за счет значительного роста накопления, обработки и распространения информации и заметного увеличения случаев киберпреступлений в отношении граждан, государства и бизнеса.

Современная киберпреступность развилась из кибермошенничества до кибершпионажа или кибертерроризма. В 2021 году 92% хакерских атак были направлены на государственные организации, предприятия военно-промышленного комплекса, энергетики и добывающей промышленности.

Создание и внедрение СОИБ в структуру предприятий нацелено на предотвращение доступа злоумышленников к обрабатываемой информации, недопущение несанкционированного воздействия, влекущего нарушение или прекращение функционирования предприятия или его части, а также оперативное восстановление функционирования ЗОКИИ после аварий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон от 26 июля 2017 г. N 187-ФЗ (последняя редакция). – Текст: электронный // ФСТЭК России: [сайт] – URL: https://clck.ru/3476gH.
2. Законодательство в сфере ИБ и цифровой экономики за 2021–2022. Текст: электронный // Infowatch: [сайт]. – URL: https://clck.ru/3476ha.
3. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 (в ред. приказов ФСТЭК России от 20 февраля 2020 г. n 35). – Текст: электронный // ФСТЭК России: [сайт] – URL: https://clck.ru/RcsYb.

Yamin Artem D.,
graduate student,
School of Management and Interdisciplinary Studies,
Department of Economics and Management,
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russian Federation

Tarasyev Alexander A.,
Candidate of Economic Sciences, Associate professor,
School of Management and Interdisciplinary Studies,
Department of Economics and Management at Systems Analysis and Decision-Making Enterprises,
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russian Federation

MECHANISMS AND PRINCIPLES OF INFORMATION SECURITY IMPLEMENTATION AT ENTERPRISES

Abstract:
The article describes the activities of the state and enterprises in the field of information security, as well as a general overview of the structure of the information security system.
As a description of the compliance of the applied protection measures, a classification of organizational and technical protection measures is presented.

Keywords:
Cyber security, information security system, cyber-attack, cybercrime, significant object of critical information infrastructure.